I-Storm ADSL Router
With Firewall Built-in

Manuale Utente (V1.41)

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni e vi preghiamo di segnalarceli. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del nostro manuale, software e/o hardware.
Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land spa che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land spa. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

FCC

Questo apparecchio è stato testato e risultato appartenente alla “Class B digital device”, in conformità alla “Part 15 delle FCC Rules”. Questi limiti sono pensati per offrire una ragionevole protezione contro dannose interferenze in ambienti di tipo domestico. Questo apparecchio genera, assorbe e può irradiare energia sotto forma di frequenze radio, se non installato e usato in conformità con le istruzioni. Questo può causare dannose interferenze ad ogni tipo di comunicazione radio. Tuttavia questa ipotesi potrebbe verificarsi anche in caso di corretta installazione in particolari situazioni, in questo caso rivolgersi a personale qualificato.

INDICE

Capitolo 1
Introduzione

1.1 Panoramica dell'I-Storm ADSL Router

L'I-Storm ADSL Router dispone di una porta per connessione ADSL ad alta velocità e una porta Ethernet. Supporta in downstream un tasso di trasmissione fino ad 8Mbps e in upstream un tasso di trasmissione sino a 1024Kbps, inoltre soddisfa il Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).

Il prodotto supporta i protocolli PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged oppure routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) e PPTP-to-PPPoA relaying per stabilire una connessione con l'ISP. Inoltre incorpora un client PPTP per stabilire una connessione VPN con un server remoto PPTP. Il prodotto supporta inoltre VC-based ed il LLC-based multiplexing.

Il prodotto è la soluzione ideale per connettere un piccolo gruppo di PC ad Internet tramite una connessione veloce ADSL. In questo modo molti utenti possono condividere questa connessione ed avere accesso simultaneamente ad Internet.

Il prodotto inoltre offre un Internet firewall adatto a proteggere la Lan locale da accessi indesiderati. Possiede oltre alla funzione di NAT, che di per sé è una sorta di prima difesa, anche tutta una serie di caratteristiche proprie che lo rendono adatto a garantire la sicurezza della Lan. Può inoltre essere configurato per impedire ad utenti interni, della Lan, di accedere ad Internet.

Il prodotto fornisce tre livelli di sicurezza. Anzitutto maschera l'indirizzo IP dell'utente della Lan, rendendolo invisibile agli utenti di Internet rendendo, in tal modo, molto più difficoltoso, per un hacker, di localizzare il PC nella Lan. Può inoltre bloccare e fare il redirect di alcune porte per limitare i servizi cui utenti esterni possono accedere. A titolo di esempio, per assicurarsi che alcuni giochi o altre applicazioni possano funzionare correttamente, è possibile aprire alcune porte specifiche per utenti esterni per consentire l'accesso a servizi forniti da PC della Lan. Infine l'I-Storm ADSL Router può smascherare e bloccare tutta una serie di Hacker Patterns non consentendo così all'hacker di accedere alla Lan, inoltre conserverà tutti questi attacchi rilevati (come qualunque pacchetto "intercettato" dal firewall) in una opportuna tabella che potrà essere poi consultata.

Il servizio DHCP è integrato, client e server, consentendo (sino ad un massimo di 253) ai PC della Lan di ricevere il loro indirizzo IP privato dinamico all'accensione in maniera del tutto automatica. E' sufficiente settare il PC come client DHCP e L'I-Storm ADSL Router provvederà a passargli tutte le informazioni necessarie (indirizzo IP, netmask, DNS, default gateway). Ogni volta che un PC viene acceso, se configurato come client DHCP, viene riconosciuto dal Router ADSL che gli assegna un IP privato istantaneamente.

Per utenti avanzati la funzione di Virtual Service offerta dal prodotto consente la visibilità alla macchina locale con uno specifico server nei confronti di utenti esterni. Un ISP fornisce un indirizzo IP che può essere assegnato al Router ADSL e gli specifici servizi possono essere rediretti ad uno specifico computer della Lan. Un server Web può essere connesso ad internet attraverso il Router

ADSL che quando riceve una richiesta di accesso, via html, rigira i pacchetti all'IP della Lan su cui è il PC che ospita il server Web. In questo caso il server Web è protetto da ogni tipo di attacchi grazie al lavoro fatto dal firewall dell'I-Storm ADSL Router.

La funzione di Virtual Service inoltre consente di reindirizzare a più di un PC diversi servizi. Per esempio è possibile rigirare separatamente servizi diversi a PC diversi che comunque restano protetti dal firewall presente sull'I-Storm ADSL Router.

1.2 Contenuto della confezione

- I-Storm ADSL Router
- CD-ROM contenente il manuale (Inglese e Italiano), le guide rapide (Inglese, Italiano e Francese) ed il firmware
- Guida di Quick Start multilingua (Inglese, Italiano e Francese)
- cavo RJ-11 ADSL
- cavo incrociato CAT-5 LAN
- cavo seriale RS232 DB9
- Alimentatore AC-DC (5V, 2.6A)

1.3 Caratteristiche dell'I-Storm ADSL Router

Caratteristiche offerte dall'I-Storm ADSL Router:

ADSL Multi-Mode Standard: Supporta in downstream un tasso di trasmissione fino 8Mbps ed un tasso di trasmissione in upstream sino a1024Kbps, inoltre soddisfa il Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).

Multi-Protocol per stabilire la connessione: Supporta PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged oppure routed), PPP over Ethernet (RFC 2516), IPoA (RFC1577) e PPTP-to-PPPoA relaying per stabilire la connessione con l'ISP. Il prodotto supporta inoltre VC-based ed il LLC-based multiplexing.

Network Address Translation (NAT): Consente a diversi utenti di accedere alle risorse esterne, come Internet, simultaneamente attraverso un indirizzo IP singolo. Sono inoltre supportate direttamente come web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting e altro.

Firewall: Supporta un SOHO firewall con tecnologia NAT. Automaticamente scopre e blocca l'attacco di tipo Denial of Service (DoS) attack. L'attacco dell'hacker è registrato e conservato in un'area protetta. Aggiornando il firmware, scaricabile dal sito www.atlantisland.it o www.atlantis-land.com, è possibile migliorare questa capacità al fine di mantenerla allineata all'evolversi della tipologia di attacchi.

Packet Filtering: Non solo filtra i pacchetti in base all'indirizzo IP ma anche in base alla porta usata (dunque il tipo di pacchetti TCP/UDP/ICMP). Questo può migliorare le prestazioni nella Lan oltre che a provvedere un controllo di alto livello.

Sicurezza nei protocolli PPPoA e PPPoE: Il Router supporta infatti i protocolli PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol).

SPI: grazie alla funzionalità di Stateful Packet Inspection il Router esamina a fondo ogni pacchetto consentendo il passaggio dei soli pacchetti ritenuti sicuri. Questa tecnica consente di evitare gli attacchi di tipo Spoofing.

Domain Name System (DNS) relay: Un Domain Name System (DNS) contiene una tabella di corrispondenze tra nomi di domini ed indirizzi IP pubblici. In Internet un certo sito ha un unico nome come www.yahoo.com ed un indirizzo IP. L'indirizzo IP è difficile da ricordare (però è assolutamente il modo più efficiente), certamente molto più del nome. Questo compito è svolto appunto dal DNS che grazie alla tabella incorporata riesce a fornire al PC che ne fa richiesta l'indirizzo IP corrispondente al nome del sito (e qualora non l'avesse la richiederà ad altri server DNS di cui conosce l'IP). Il Router ricevuto il pacchetto lo rigira al PC che ne ha fatto richiesta.

Virtual Private Network (VPN): Permette all'utente di creare un tunnel direttamente per garantire connessioni sicure. L'utente può usare il client PPTP supportato dall'I-Storm ADSL Router per creare una connessione VPN oppure lanciare il client PPTP da un PC ed il Router consente il passaggio di IPSec e PPTP.

Virtual Private Network (VPN IPSec): Permette all'utente di creare un tunnel direttamente per garantire connessioni sicure. L'utente può usare direttamente il Router per accettare o chiamare un altro Router ed effettuare così VPN in IPSec che consentono a LAN diverse di dialogare in tutta sicurezza.

PPP over Ethernet (PPPoE): Offre il supporto per stabilire connessioni, con l'ISP, che usano il protocollo PPPoE. Gli utenti possono avere un accesso ad Internet ad alta velocità di cui condividono lo stesso indirizzo IP pubblico assegnato dall'ISP e pagano per un solo account. Non è richiesto nessuno client software PPPoE per i PC locali. Sono inoltre offerte funzionalità di Dial On Demand e auto disconnection (Idle Timer).

Virtual Server: L'utente può specificare alcuni servizi che si rendono disponibili per utenti esterni. L'I-Storm ADSL Router può riconoscere le richieste entranti di questi servizi e rigirarle al PC della Lan che li offre. E' possibile, per esempio, assegnare una data funziona ad un PC della Lan (come server Web) e renderlo disponibile in Internet (tramite l'unico IP statico disponibile). Dall'esterno è così possibile accedere al server Web che resta comunque protetto dal NAT.

Dynamic Host Control Protocol (DHCP) client and server: Nella WAN, DHCP client può prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della Lan.

Protocollo RIP1/2 per il Routing: Supporta una semplice tabella statica oppure il protocollo RIP1/2 per le capacità di routing.

SNTP: Una facile via per avere informazioni sull'ora dal server SNTP.

Configurabile (GUI) via Web: la gestione e la configurazione sono possibili via interfaccia grafica (browser). Dispone di un comodo help in linea che aiuta l'utente. Supporta inoltre la funzione di management remota con la quale è possibile configurare e gestire il prodotto.

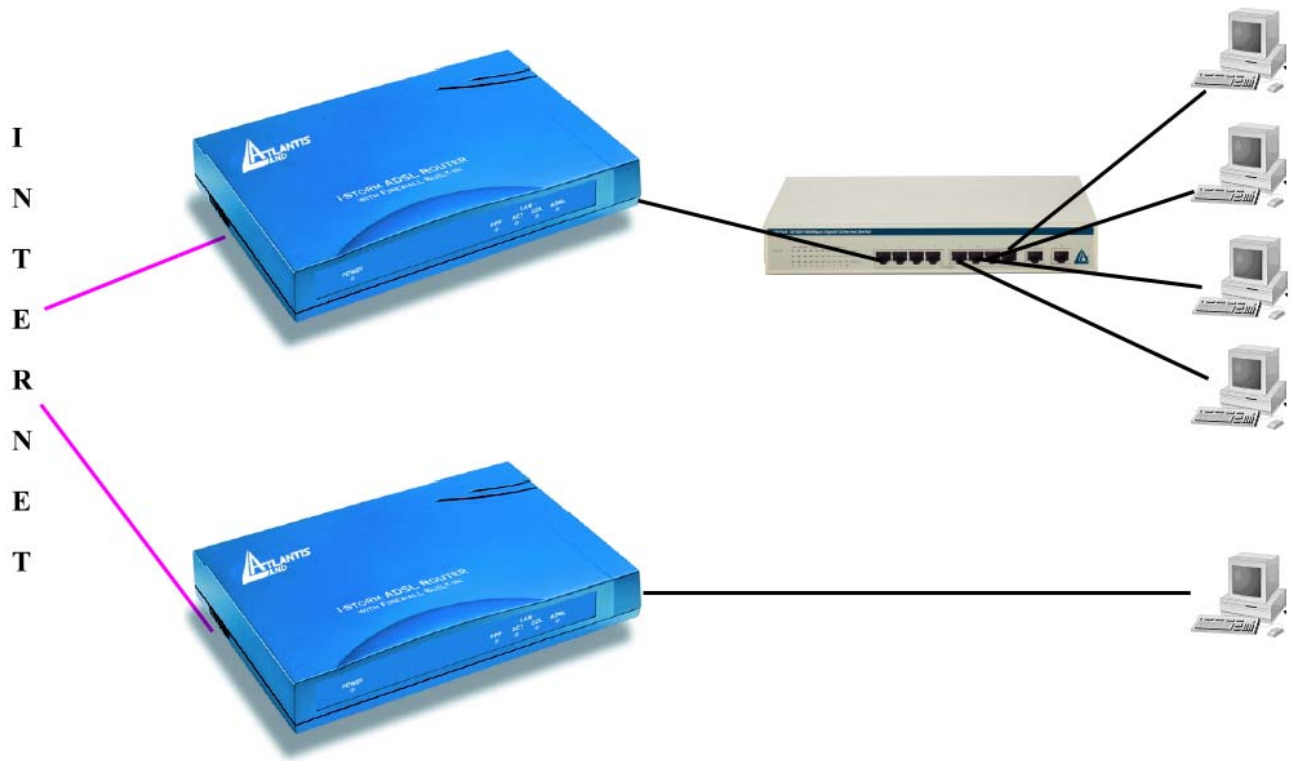
1.4 Schema di installazione dell'I-Storm ADSL Router

A) Collegare la porta WAN (*LINE*) alla linea telefonica per mezzo del cavo RJ11 (in dotazione)
B) L'I-Storm Router ADSL può essere collegato, tramite la porta RJ45 (*LAN*), nelle seguenti modalità:

- Direttamente ad un **PC**, tramite il cavo CAT 5 **incrociato** (in dotazione).
- Ad un **Hub/Switch** nella **porta UPLINK** con il cavo CAT 5 **incrociato** (in dotazione).
- Ad un **Hub/Switch** con un cavo CAT 5 **diritto**.

C) Collegare l'alimentatore AC-DC (2.6A, 5V) alla rete elettrica e all'apposito attacco (*POWER*) situato nel pannello posteriore.
D) E' possibile collegare l'I-Storm Router ADSL ad un PC tramite il cavo RS232 (in dotazione tipo DB9-DB9) per configurarlo tramite la Console.

E' possibile vedere in figura un esempio di cablaggio di una rete (parte superiore) , si ricorda che è possibile usare l'I-Storm ADSL router anche con un solo PC e senza hub/switch collegandolo direttamente alla scheda di rete col cavo fornito in dotazione (parte inferiore).



Capitolo 2
Uso dell'I-Storm ADSL Router

2.1 Precauzioni nell'uso dell'I-Storm ADSL Router

Non usare il Router ADSL in un luogo in cui ci siano condizioni di alte temperatura ed umidità.

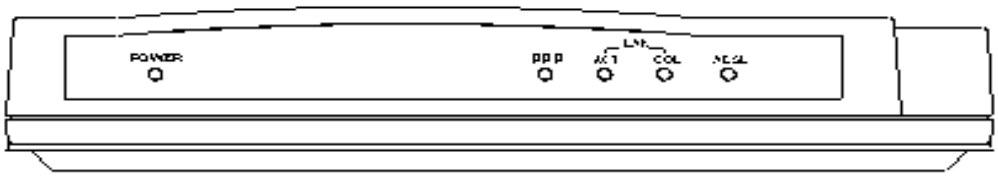
Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori del Router ADSL.

Non aprire mai il case del Router ADSL né cercare di ripararlo da soli . Se il Router ADSL dovesse essere troppo caldo, spegnerlo immediatamente e rivolgersi a personale qualificato.

Mettere il Router ADSL in una superficie piana e stabile.

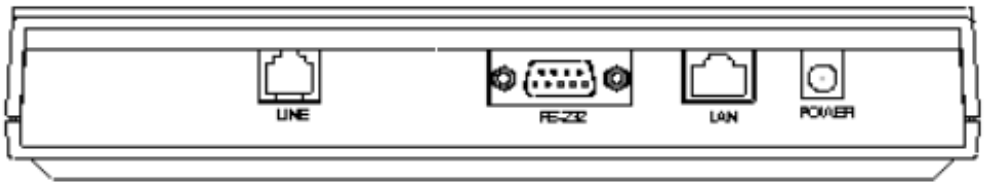
Usare esclusivamente l'alimentatore fornito nella confezione.

2.2 I LED frontali



LED		Informazione
1	**Power**	Acceso fisso quando connesso alla rete elettrica
2	**PPP**	Acceso fisso quando una connessione PPPoE / PPPoA è attiva. Lampeggia quando tenta di costruire una connessione PPP. Spenta se si utilizza un protocollo diverso (RFC 1483 o 1577)
3	**LAN / ACT**	Acceso fisso quando connessa alla LAN Lampeggia quando manda/riceve dati
4	**LAN / COL**	Acceso fisso in presenza di collisioni.
5	**ADSL**	Acceso fisso quando connesso in modalità ADSL DSLAM.

2.3 Le PORTE posteriori



Porte		Utilizzo
1	**Power (jack)**	Connettere l'alimentatore a questo jack
2	**LAN (RJ-45 connettore)**	Connesso con un cavo Ethernet **incrociato** (quello fornito) quando è connesso alla scheda Lan (del PC) o nella porta uplink dell'hub/switch. Connesso con un cavo Ethernet **dritto** quando è connesso alla Lan (hub o switch, non nella porta uplink)
3	**RS-232 (porta)**	Connettere il cavo RS232 fornito alla porta seriale (9 pin) del PC. Tale connessione è opzionale.
4	**LINE (RJ-11 connettore)**	Connettere il cavo RJ-11 a questa porta per effettuare l'allacciamento all'ADSL.

2.4 Cablaggio

Il problema più comune è quello di un cattivo cablaggio per Ethernet o per la Lan. Accertarsi che tutti i dispositivi connessi siano accesi, usare inoltre i Led frontali per avere una diagnosi immediata dello stato del cablaggio. Controllare che siano accesi sia il Led Lan che quello ADSL (qualora così non fosse ricontrollate il cablaggio). Il cavo deve essere incrociato se il dispositivo è connesso direttamente ad un PC, nel caso invece in cui sia connesso ad un Hub/Switch usare un cavo diritto, usare invece un cavo Ethernet di tipo incrociato se collegato alla porta uplink.

L'I-Storm ADSL Router non è in grado di accorgersi se il cablaggio è corretto. Accertarsi di usare il cavo corretto a seconda che il dispositivo sia connesso ad un PC o un Hub/Switch. Accertarsi che il cavo che collega l'I-Storm ADSL Router, qualora non sia quello in dotazione, sia di Cat 5 e di lunghezza inferiore a 100 metri.

Poiché l'ADSL ed il normale servizio telefonico si dividono (spesso) lo stesso filo per trasportare i rispettivi segnali è necessario, al fine di evitare interferenze dannose, dividere tramite un apposito filtro i 2 segnali. Tale filtro passa basso permetterà di estrarre la porzione di spettro utilizzata dal servizio telefonico impedendo così che la qualità di questo sia compromessa dalle alte frequenze introdotte dal segnale dell'ADSL. E' necessario pertanto utilizzare un filtro per ogni presa cui è attaccato un telefono analogico. Esistono opportuni filtri che dispongono di 2 uscite (una PSTN ed una ADSL) e consentono di utilizzare sulla stessa presa sia un telefono analogico che il Router ADSL. Tale filtro non è compreso col prodotto e va acquistato separatamente.

Capitolo 3
Configurazione

L'I-Storm ADSL Router può essere configurato col browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet. Il prodotto offre un'interfaccia molto amichevole per la configurazione.

3.1 Prima di iniziare

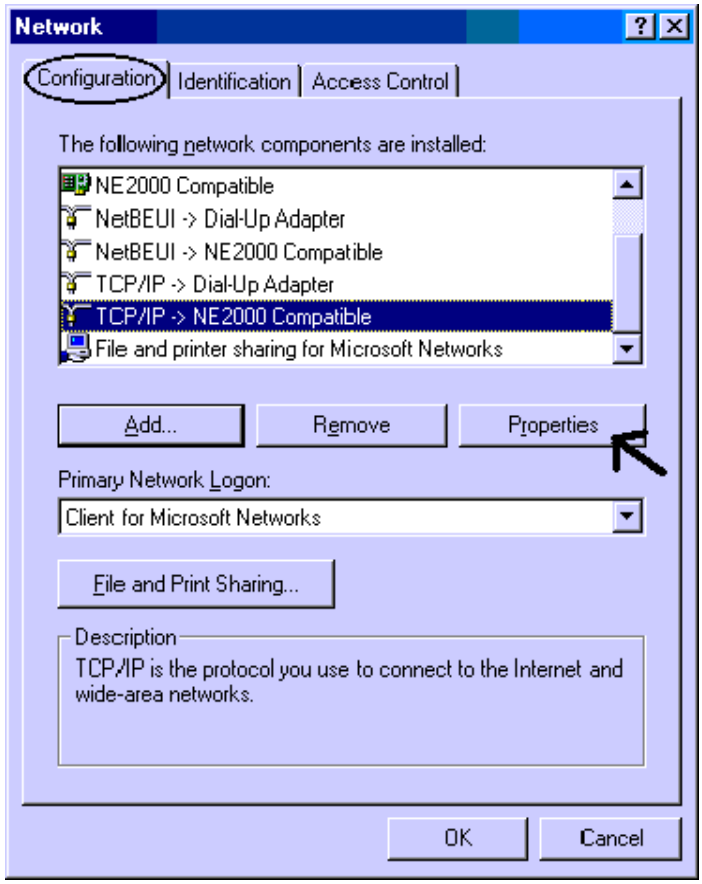
Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è connesso il Router ADSL. Tutti i PC devono avere una scheda di rete Ethernet installata correttamente, essere connessi al Router ADSL direttamente o tramite un Hub/Switch ed avere il protocollo TCP/IP installato e correttamente configurato in modo da ottenere un indirizzo IP tramite il DHCP, oppure un indirizzo IP che deve stare nella stessa subnet del Router ADSL. L'indirizzo IP di default è 192.168.1.254 e subnet mask 255.255.255.0. Certamente la strada più semplice per configurare i PC è quella settarli come client DHCP cui l'IP (ed altri parametri) è assegnato dal Router ADSL.

Anzitutto è necessario preparare i PC inserendovi (qualora non ci fosse già) la scheda di rete. E' necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:

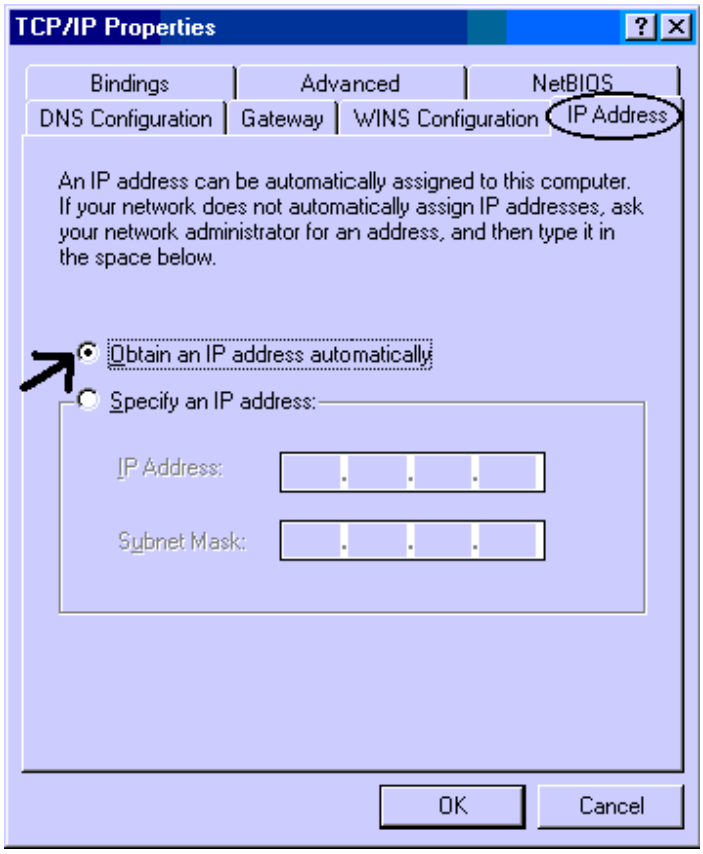
Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite il Router ADSL. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

Configurazione del PC in Windows 95/98/ME

1. Andare in **Start/Settings/Control Panel**. Cliccare 2 volte su **Network** e scegliere **Configuration**.
2. Selezionare **TCP/IP -> NE2000 Compatible**, o qualsiasi Network Interface Card (NIC) del PC.
3. Cliccare su **Properties**.

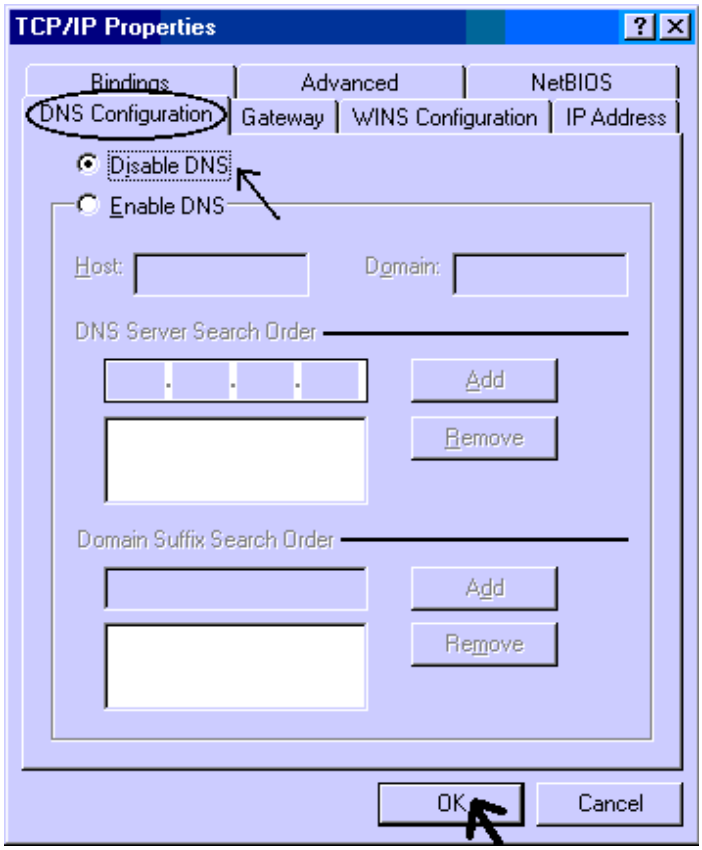


4. Selezionare l'opzione **Obtain an IP address automatically** (dopo aver scelto **IP Address**).



5. Andare su **DNS Configuration**

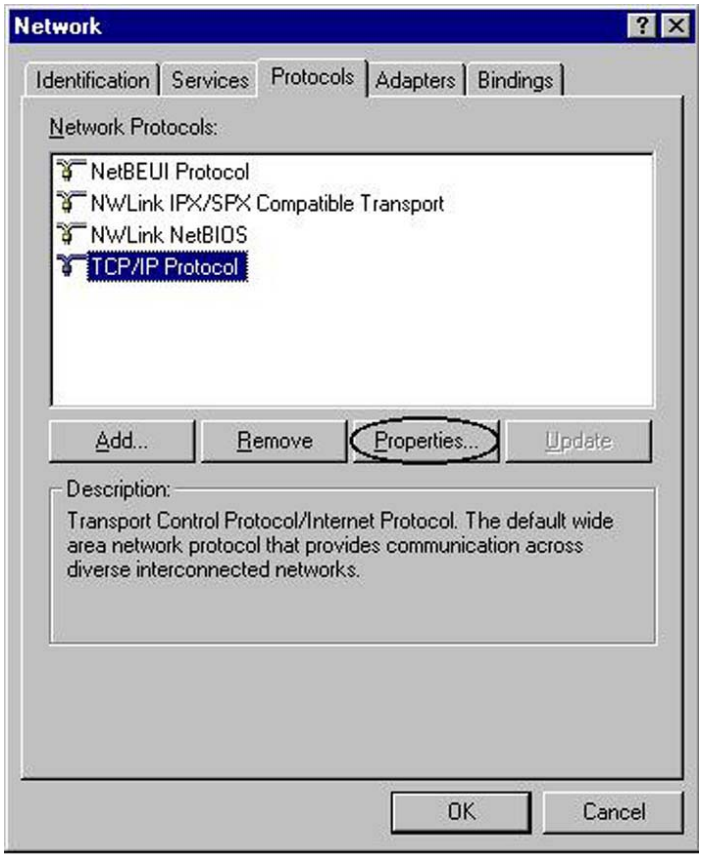
6. Selezionare l'opzione **Disable DNS** e premere su **OK** per terminare la configurazione.



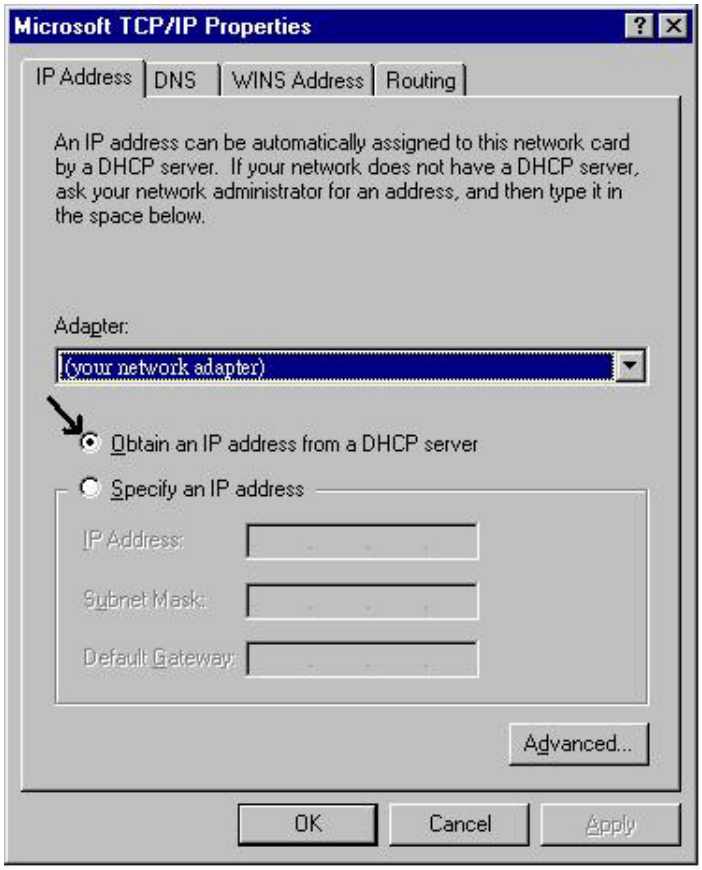
Configurazione del PC in Windows NT4.0

1. Andare su **Start/Settings/ Control Panel**. Cliccare per due volte su N**etwork** e poi cliccare su **Protocols** .

2. Selezionare **TCP/IP Protocol** e poi cliccare su **Properties**.

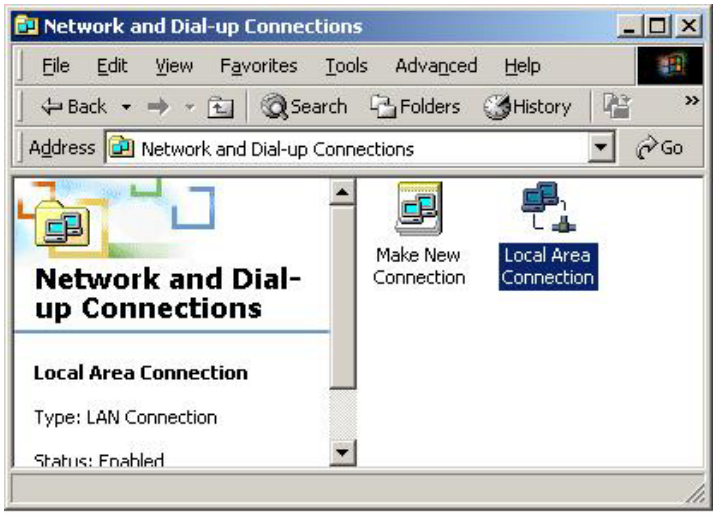


3. Selezionare l'opzione **Obtain an IP address from a DHCP server** e premere **OK**.

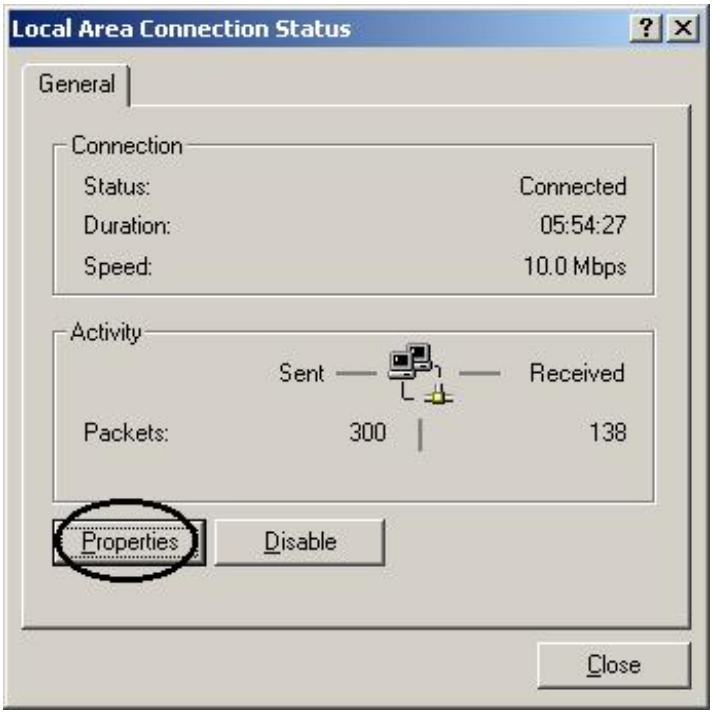


Configurazione del PC in Windows 2000

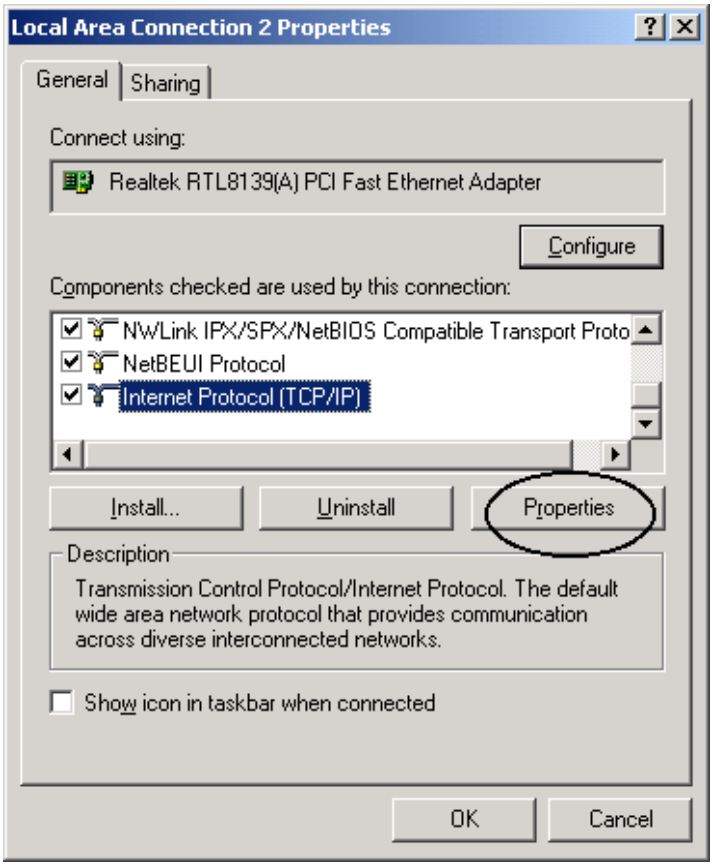
1. Andare su **Start/Settings/Control Panel**. Cliccare due volte su **Network and Dial-up Connections**.
2. Cliccare due volte su **Local Area Connection**.



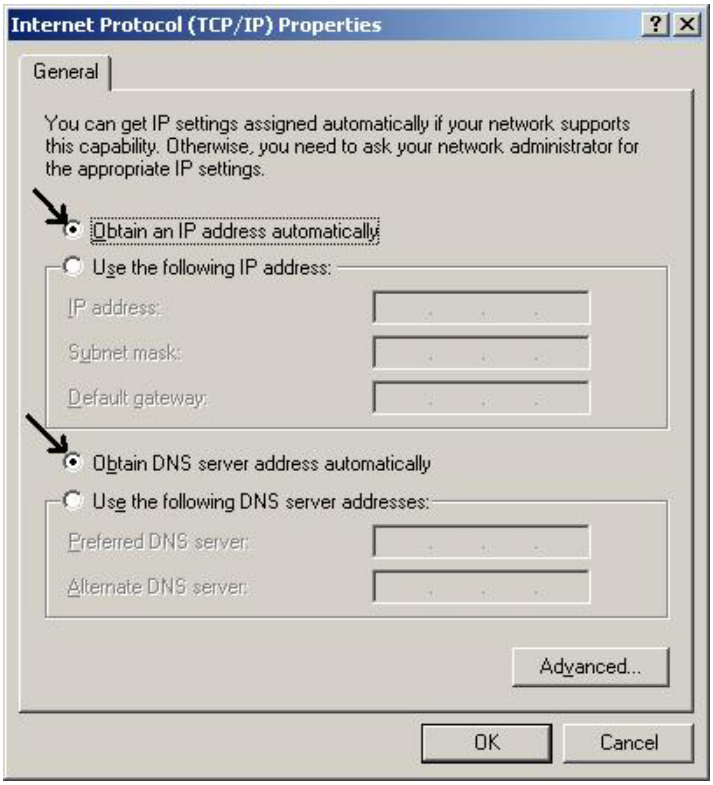
3. In **Local Area Connection Status** cliccare **Properties**.



4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.

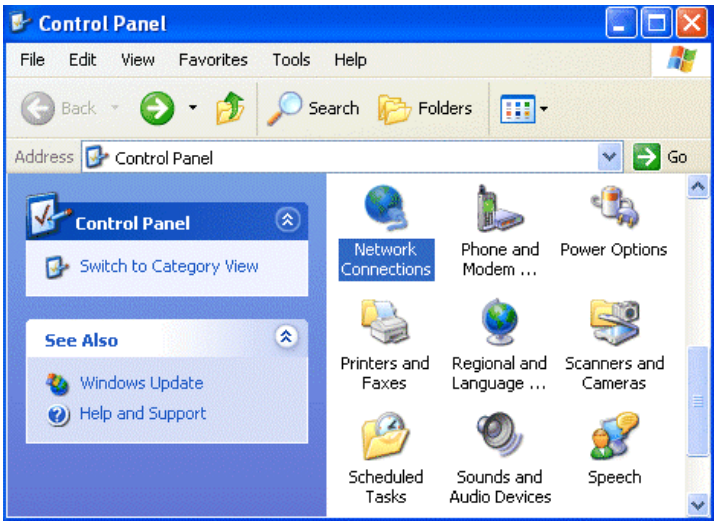


5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically**
6. Premere su **OK** per terminare la configurazione

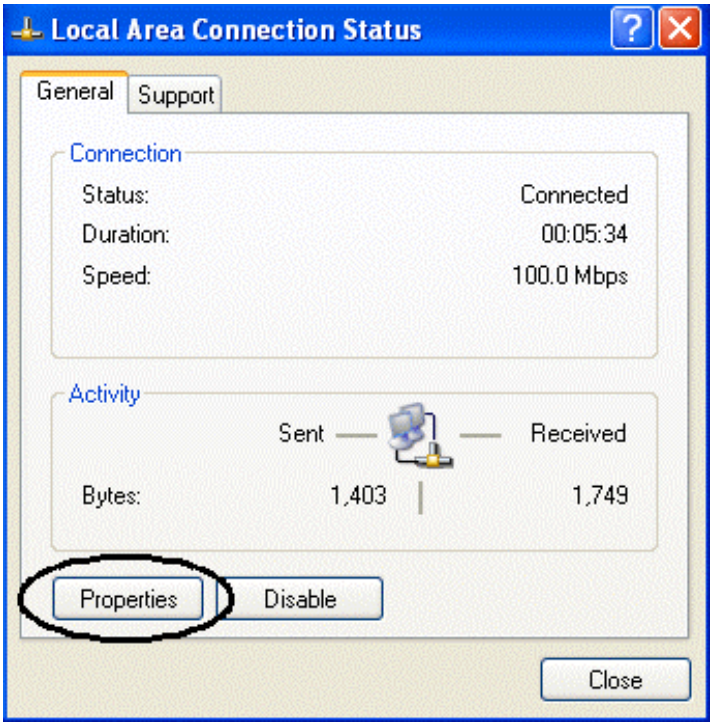


Configurazione del PC in Windows XP

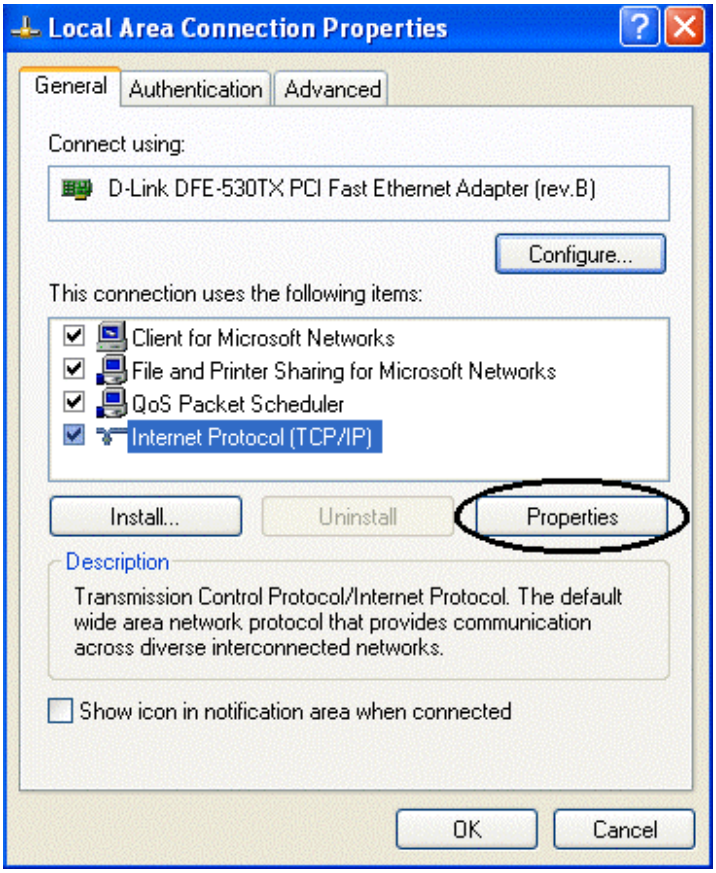
1. Andare su **Start** e poi **Control Panel**. Cliccare due volte su **Network (in Classic View) Connections**.
2. Cliccare due volte su **Local Area Connection**.



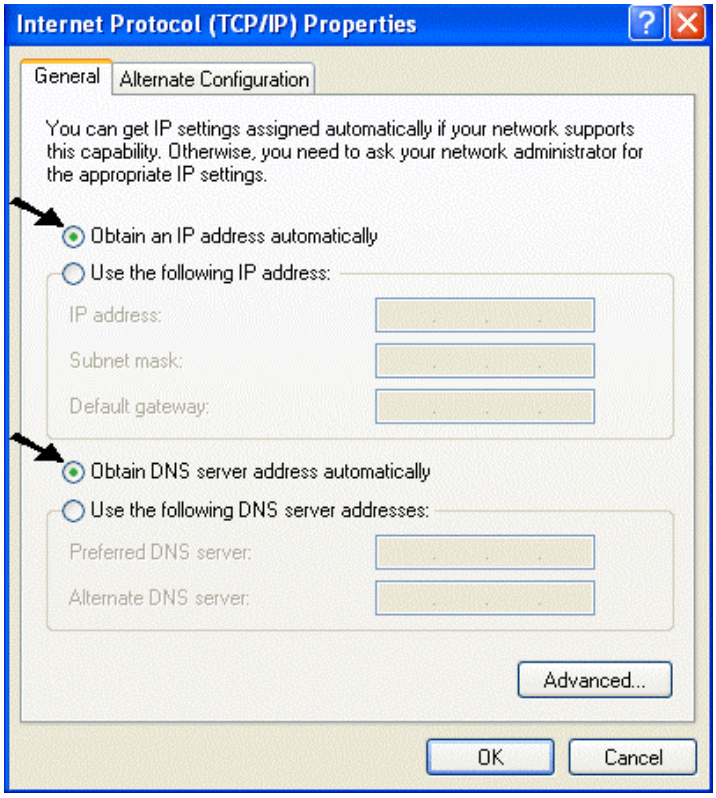
3. In **Local Area Connection Status** cliccare **Properties**.



4. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.

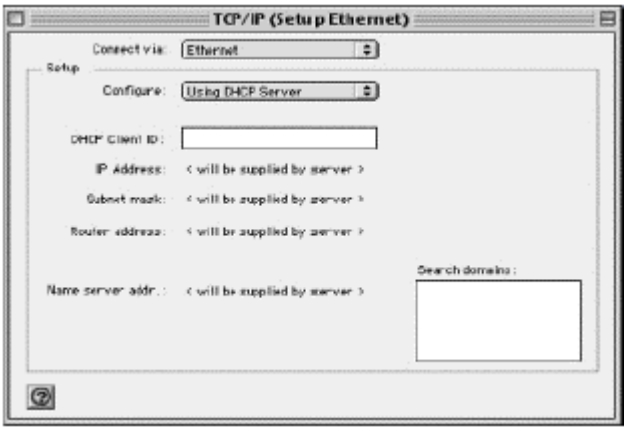


5. Selezionare l'opzione **Obtain an IP address automatically** e successivamente **Obtain DNS server address automatically** .
6. Premere su **OK** per terminare la configurazione.



Configurazione in ambiente MAC

1. Cliccare sull'**icona Mela** nell'angolo in alto a sinistra dello schermo e selezionare: **Control Panel/TCP/IP**. Apparirà la finestra relativa al TCP/IP come mostrata in figura.
2. Scegliere **Ethernet** in **Connect Via**.
3. Scegliere **Using DHCP Server** in **Configure**.
4. Lasciare vuoto il campo **DHCP Client ID**.

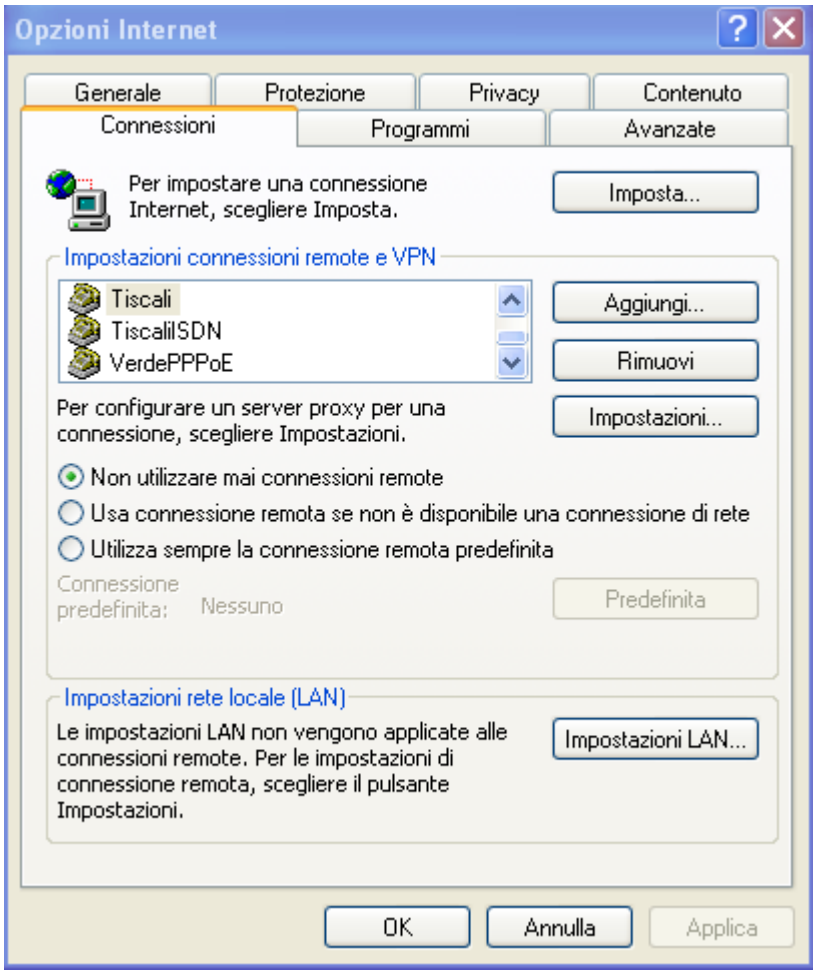


3.1.1 Configurazione del Browser

A questo punto è necessario lanciare IE, andare nel menù **strumenti,** poi scegliere il tab **connessioni** e scegliere le voci:

- non utilizzare mai connessione remota
- usa connessione remota se non è disponibile una connessione di rete

Si osservi la figura sottostante.



3.2 Settaggi di Default

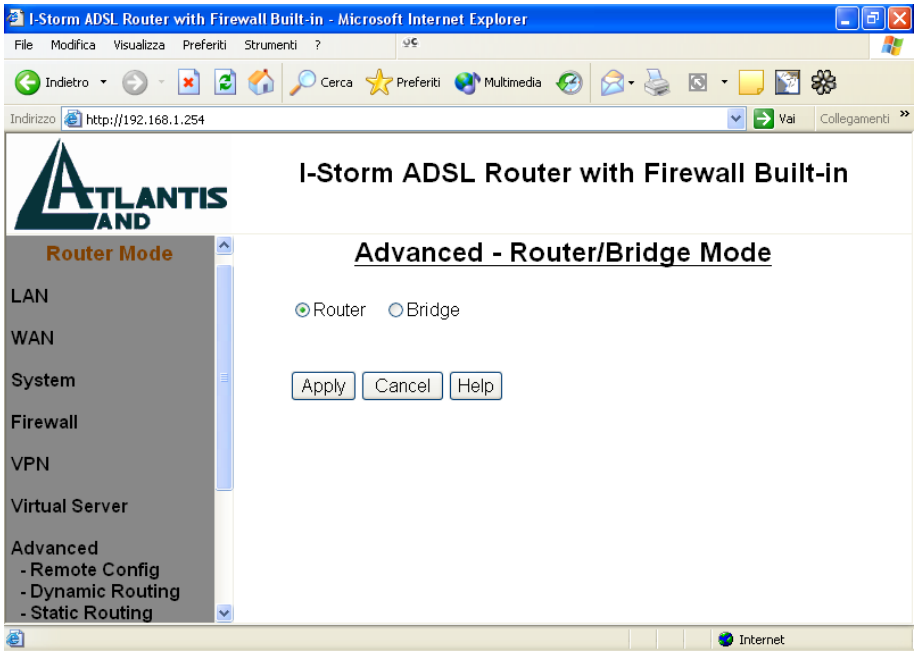
Prima di iniziare la configurazione dell'I-Storm ADSL Router è necessario conoscere quali siano i settaggi di default:

- **Web Configurator**
  Password : <BLANK>, BLANK inteso nel senso di non introdurre alcun carattere.
- Indirizzo IP e subnet Mask
  IP Address : 192.168.1.254
  Subnet Mask : 255.255.255.0
- **Router/Bridge modalità**=Router
- **ISP setting in WAN site**
  PPPoE (VCI=8, VPI=35)
- **DHCP server**

DHCP server è abilitato.
Indirizzo IP di partenza : 192.168.1.100
IP abilitati : 100

3.2.1 Modalità Router/Bridge

La modalità di default è **Router**. Per cambiare tra le 2 modalità ciccare in **Advanced → Router/Bridge Mode** a sinistra nel Menù Principale. Selezionare la modalità che si preferisce usare e premere sul bottone **Apply.**



3.2.2 Password

La password di default non è definita (nessun carattere), premere invio per entrare immediatamente. Quando si configura l'I-Storm ADSL Router con il browser premere su **OK** per entrare per la prima volta. E' consigliato cambiare la password, al fine di aumentare la sicurezza. L'I-Storm ADSL Router conserva una sola password per volta.

Qualora si perdesse la password consultare la sezione opportuna nel capitolo 4.

3.2.3 Porte LAN e WAN

I parametri della Lan e wan sono settati di default nella seguente maniera:

Porta LAN		Porta WAN
IP address	192.168.1.254	Il Protocollo PPPoE è settato come default per la connessione con l'ISP (serve solamente la Password e Username).
Subnet Mask	255.255.255.0	
Funzionalità DHCP server	Abilitato	
Indirizzi IP distribuiti ai PC	100 IP disponibili da 192.168.1.100 sino a 192.168.1.199 (Attualmente sono supportati sino a 253 utenti.)	

3.3 Informazione sull'ISP

Prima di iniziare la configurazione dell'I-Storm ADSL Router è necessario ricevere dal proprio ISP il tipo di protocollo supportato per la connessione (PPPoE, PPPoA, RFC1483, IPoA, oppure PPTP-to-PPPoA Relaying).

Può essere utile, prima di iniziare, accertarsi di avere le informazioni riportate nella tabella sottostante:

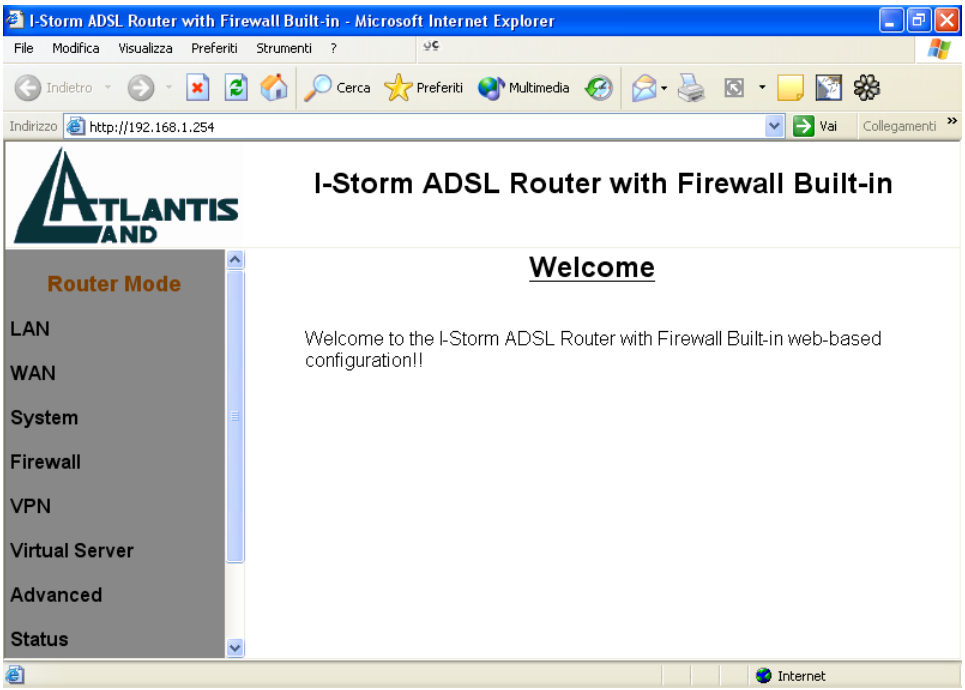
PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name e indirizzo IP del Domain Name System (DNS) (può essere assegnato dall'ISP in maniera dinamica, oppure fisso).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing e configurare il dispositivo in BRIDGE.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing,indirizzo IP, Subnet mask, Gateway address, e indirizzi IP dei Domain Name System (DNS, sono IP fissi).
IPoA	VPI/VCI, IP address, Subnet mask, indirizzo del Gateway, e e indirizzi IP dei Domain Name System (DNS, sono IP fissi).
PPTP-to-PPPoA Relaying	VPI/VCI, VC-based/LLC-based multiplexing, e indirizzi IP dei Domain Name System (DNS, sono IP fissi).

3.4 Configurazione col Browser in modalità Router

Accedere col browser web al seguente indirizzo IP (dove si inserisce l'URL) che di default è: **192.168.1.254**, e premere il tasto invio.

Nessun User Name o Password è richiesta (nel caso di primo accesso). Qualora la password fosse stata cambiata bisogna invece inserirla. Premere **OK** per continuare.

Apparirà a questo punto il Menù Principale, nella parte sinistra si potrà accedere (come se si stessero vedendo i links in una homepage) a tutte le sezioni: **LAN, WAN, System, Firewall, VPN, Virtual Server, Advanced, Status, Help** ed infine **Logout**.

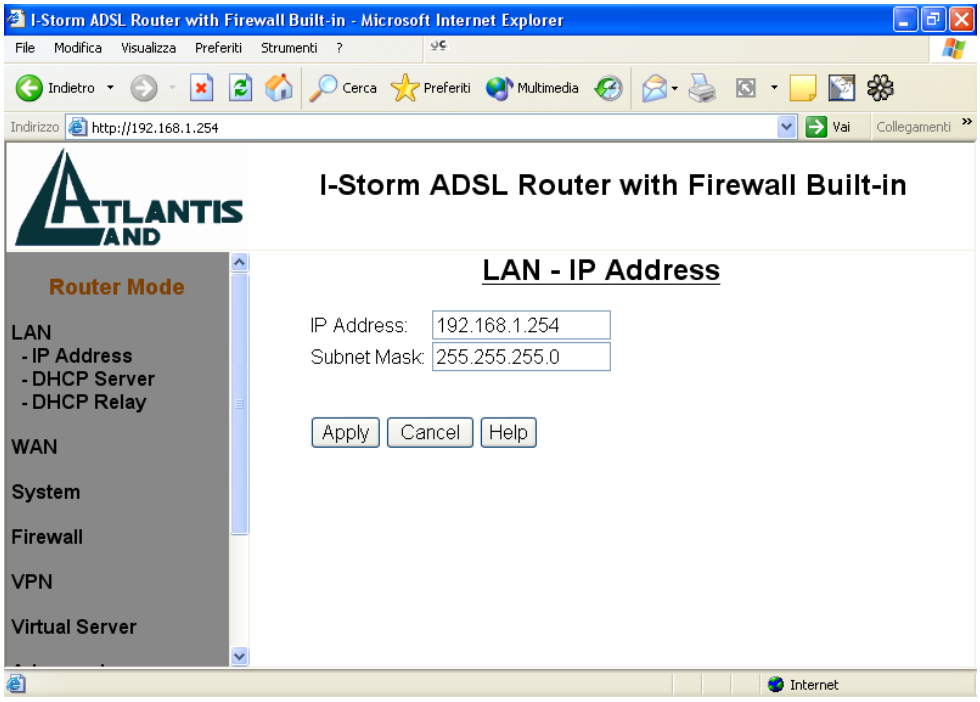


Cliccando sulla sezione desiderata, si vedrà nello spazio della homepage tutti i settaggi relativi alla configurazione della sezione scelta, oppure si apriranno tutta una serie di sottosezioni tra cui scegliere prima di avere accesso alle configurazione vere e proprie.

3.4.1 LAN

Questa sezione contiene i settaggi per la LAN interna. Selezionandola appariranno 3 nuove sottosezioni: **IP Address, DHCP Server e DHCP relay.**

IP Address



IP Address: Il valore di default è:**192.168.1.254**

Questo è l'indirizzo IP con cui l'I-Storm ADSL Router è visto nella LAN (potrebbe essere un IP pubblico nel caso l'ISP vi fornisca una classe). E' necessario, qualora si cambiasse IP con quello di un'altra subnet accertarsi che tutti i PC della LAN abbiano un indirizzo IP (se non sono settati come client DHCP) nella stessa subnet. Diversamente questo potrebbe impedire il corretto funzionamento della LAN e l'accesso al Router ADSL.

Subnet Mask: Il valore di default è:**255.255.255.0**

Gli scenari possibili per la configurazione di una rete Lan privata (o pubblica) ed il Router ADSL potrebbero essere moltissimi, a titolo d'esempio vengono riportati i più comuni. Quando si implementa il Nat si isola di fatto la propria Lan da Internet. La Lan locale, se privata, deve avere gli indirizzi IP appartenenti ai seguenti blocchi (riservati dall'ente IANA per reti private).

CLASSE	IP Partenza	IP Finale	Subnet Mask
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

E' chiaramente raccomandato scegliere gli indirizzi della propria Lan appartenenti alla tabella di sopra (per ulteriori informazioni fare riferimento all'RFC 1597).

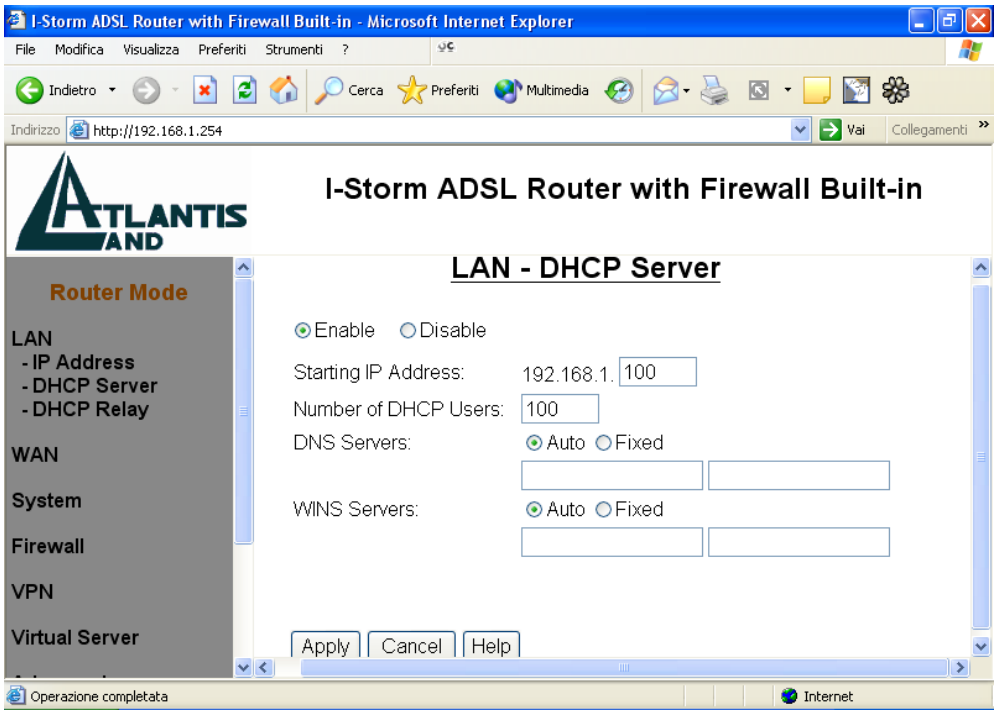
-PC con IP appartenenti ad una classe privata, il cui default gateway è il Router ADSL che fa NAT. Può essere attivo o meno il DHCP (il Router prenderà dall'altra parte un indirizzo IP pubblico statico o dinamico, ma pubblico, ed avrà un suo default Gateway che può essergli dato in automatico o settato a mano su informazione dell'ISP). Il management del Router può essere fatto da un qualunque PC collegato ad Internet (abilitando l'apposita funzione sull'I-Storm ADSL Router) oppure dai PC della Lan. Il collegamento con l'ISP può essere uno qualsiasi tra quelli supportati (il default gateway del Router ADSL sarà dato automaticamente come i DNS in caso di PPPoE e PPPoA, bisognerà inserirli in caso di altri protocolli come RFC1483). In questo caso dunque la configurazione della LAN sarebbe la seguente:

Host	Indirizzo IP	Maschera	Gateway	DNS
Router Lan IP	192.168.1.254	255.255.255.0		
PC A	192.168.1.1	255.255.255.0	192.168.1.254	Forniti ISP
PC B	192.168.1.2	255.255.255.0	192.168.1.254	Forniti ISP
PC C	192.168.1.3	255.255.255.0	192.168.1.154	Forniti ISP
PC X	192.168.1.n	255.255.255.0	192.168.1.254	Forniti ISP

In questo caso si è scelto di mantenere la rete 192.168.1.x e l'indirizzo IP (per l'I-Storm ADSL Router) di default. E' possibile in questo caso abilitare il DHCP server del Router ma bisogna prestare attenzione nello scegliere un pool di indirizzi compatibile (in questo caso bisognerà settare come IP starting 192.168.1.n+1, dove n+1<254). E' comunque possibile cambiare la rete in un'altra rete (sempre appartenente alla classe B) tipo 192.168.4.x in questo caso bisognava assegnare a tutti i PC ed al Router un indirizzo IP appartenente alla rete in questione (evitando come al soliti assegnamenti doppi)

-PC con IP appartenenti ad una classe pubblica, in questo caso tutti i PC della Lan sono raggiungibili da Internet e l'interfaccia Lan del modem ha anch'essa un indirizzo IP pubblico. Il default gateway dei PC è l'IP della Lan del Router che avrà chiaramente sia il DHCP che il NAT disabilitati. L'interfaccia WAN del Router prenderà un IP che può essere pubblico o privato (si ottiene per il fornitore del servizio un risparmio di indirizzi IP), l'ISP fornirà comunque l'indirizzo del default gateway dell'I-Storm ADSL Router assieme alla subnet mask. Questo scenario è tipico con l'uso del protocollo RFC 1483 o RFC 1577. Come già accennato è possibile che il Router ADSL sia collegato (per la parte WAN) con una punto-punto composta da indirizzi IP che possono essere pubblici o privati.

DHCP Server



⊙ **Disable:** Selezionare per NON usare il DHCP Server nel Router che dunque non distribuirà gli indirizzi IP ai vari clients DHCP. In questo caso bisogna assegnare a tutti i PC della rete un indirizzo IP (diverso per ogni PC), la subnet mask, DNS e l'indirizzo del gateway (che, salvo casi particolari, dovrebbe essere quello dell'I-Storm ADSL Router).

⊙ **Enable:** Selezionare per usare il DHCP Server nel Router che dunque distribuirà gli indirizzi IP, subnet mask, gateway (l'indirizzo IP del Router) e DNS ai vari clients DHCP. Appariranno i seguenti campi:

Starting IP Address: Introdurre l'indirizzo IP di partenza del pool che il server DHCP assegnerà ai vari client**.** Il valore di default è**: 192.168.1.100**.

Number of DHCP users: Introdurre il numero massimo di computer che possono ricevere via DHCP l'indirizzo IP (gateway,DNS..). Tale valore deve essere coerente con l'indirizzo IP di partenza (se si sceglie come **Starting IP Address: 192.168.1.150** non si potrà superare come **Number of DHCP users** :**105)**.Il valore di default è **100**.

Ai PC della LAN possono però essere associati IP in maniera casuale (appartenenti al range settato).

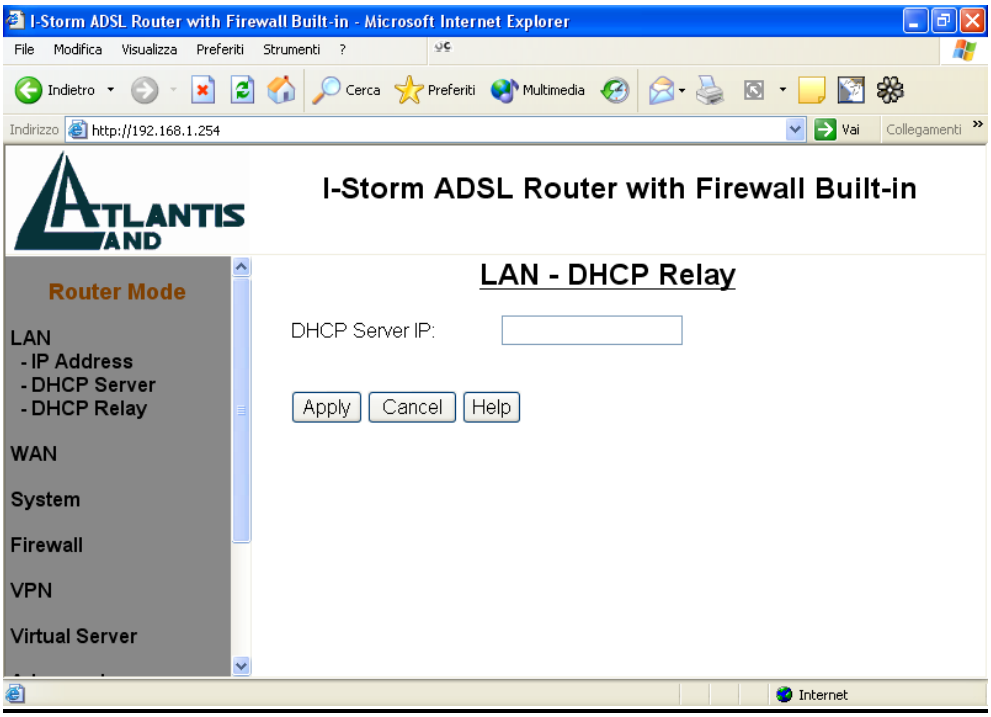
Qualora per particolari esigenze la vostra classe privata sia una classe A,B o C ma diversa dalla 192.168.1.x il Router non può fungere da server DHCP che è limitato alla classe C 192.168.1.x. In questo caso è necessario disabilitare la funzionalità DHCP dal Router. Dalla versione di Firmware 2.24 in avanti invece il DHCP sarà abilitabile anche con una classe diversa dalla 192.168.1.x.

Qualora fosse già presenti nella LAN un server DHCP bisogna disabilitare tale funzionalità nel Router ADSL (o nel PC che opera dea server DHCP) per evitare possibili conflitti.

E' inoltre possibile settare le informazioni da passare ai client DHCP sia per gli indirizzi di eventuali server wins che DNS.

DHCP Relay

Settando questa funzionalità il servizio DHCP passa attraverso il Router I-Storm e raggiunge altri server che assegnano alla Lan i vari indirizzi IP. Se questa funzionalità non fosse disponibile questi PC sarebbero impossibilitati ad accedere al server DHCP. Al solito ogni PC che necessità di un indirizzo IP si mette in contatto con un server DHCP (in questo caso fuori dalla LAN) e da questo riceve: IP, Subnet. DG, DNS. Questi indirizzi IP sono dinamici, nel senso che hanno un tempo di validità. Scaduto questo termine il client DHCP ricontatterà il server per riottenere un nuovo IP.



3.4.2 WAN

Questa sezione contiene i settaggi per la WAN . Selezionandola appariranno 2 nuove sottosezioni:**ISP** e **DNS**.

ISP

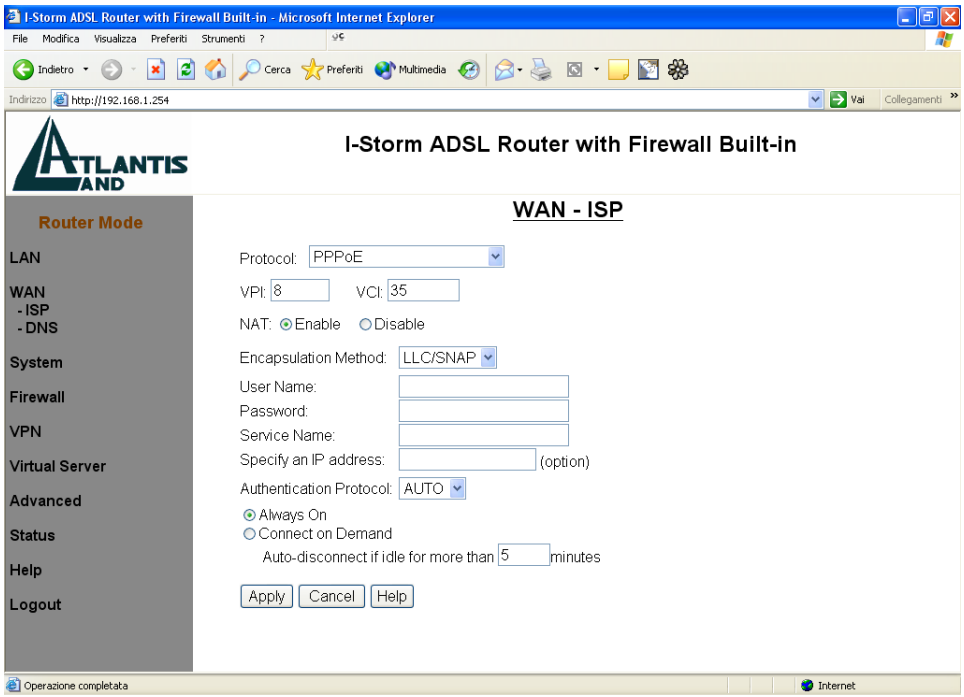
Sono disponibili cinque diverse soluzioni per la connessione con l'ISP (PPPoE, PPPoA, RFC1483 routed, IPoA, PPTP-to-PPPoA Relaying). E' necessario conoscere quale protocollo è adottato dal vostro provider.
VPI/VCI: Consultare il vostro ISP per conoscere i valori del Virtual Path Identifier (VPI) e del Virtual Channel Identifier (VCI). Il range valido per il VPI va da 0 a 255 e per il VCI da 32 a 65535. I valori di default per il VPI è 8 e per il VCI è 35.

NAT: : Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Il Nat inoltre è una sorta di primo firewall che migliora la sicurezza della Lan locale. Andrebbe usata quando il traffico indirizzato verso Internet è una parte di quello che circola nella Lan locale, altrimenti tale funzionalità potrebbe degradare leggermente le prestazioni della connessione ad Internet. Tale funzionalità coesiste con la funzionalità Virtual Server, DMZ e DHCP. Il Nat manipola i pacchetti IP uscenti e ne cambia il campo "IP provenienza" sostituendo il mittente del pacchetto (in questo caso l'indirizzo IP il PC della Lan, che è un IP privato non valido in Internet) con l'IP pubblico dell'I-Storm ADSL Router. In questo modo tutti i pacchetti uscenti dal Router avranno nel campo mittente l'indirizzo IP pubblico del Router. Quando poi i pacchetti torneranno al Router (perché sono a lui indirizzati) questo in base a tabelle memorizzate provvederà al processo contrario e li spedirà al PC interessato nella Lan.

Encapsulation Method: Assicurarsi di usare lo stesso metodo di incapsulamento usato dall'ISP (LLC/SNAP or VC MUX).

Qualora si disabilitasse la funzionalità NAT il Virtual Server e VPN saranno disabilitate.

PPPoE



PPPoE (PPP over Ethernet) è una connessione ADSL conosciuta come dial-up DSL. E' stata concepita per integrare servizi a banda larga con un'attenzione particolare alla facilità di configurazione. L'utente può beneficiare di una grande velocità di accesso senza cambiare l'idea di funzionamento, condividere lo stesso account con l'ISP. Non è richiesto alcun software aggiuntivo.

NAT: Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata.

Username: Introdurre l'username fornita dal vostro ISP. Tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.

Password: Introdurre la password fornita dal vostro ISP. Tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.

Service Name: E' un identificativo, può essere richiesto da alcuni ISP (che provvederanno a informarvi). Al solito può essere composto da massimo 63 caratteri (case sensitive) alfanumerici.

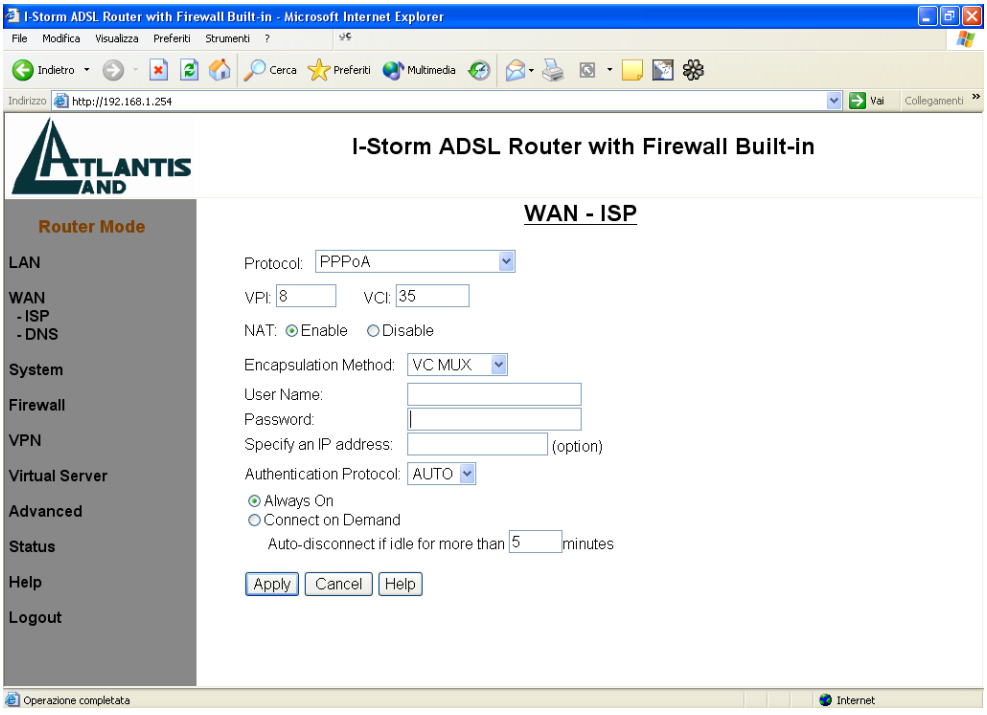
Authentication Protocol: Di default è: "AUTO". Le altre opzioni possibili sono CHAP e PAP, in caso di dubbio lasciare il valore di default.

⊙ **Always On:** Scegliere questa opzione se si desidera stabilire una sessione PPPoE nel momento dello starting up. Inoltre viene automaticamente ristabilita la connessione PPPoE qualora si venga disconnessi dall'ISP (o per ragioni tecniche la connessione cada).

⊙ **Connect on Demand:** Scegliere questa opzione se si vuole stabilire una connessione PPPoE solo quando ci sono pacchetti diretti verso Internet.

Auto-disconnect if idle for more than ☐ minutes: Disconnette automaticamente il Router ADSL quando non rileva alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore può essere settato da 0 a 999, come default è 5.

PPPoA



NAT: Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata.

Username: Introdurre l'username fornita dal vostro ISP. Tale username può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.

Password: Introdurre la password fornita dal vostro ISP. Tale password può essere composta da massimo 63 caratteri (case sensitive) alfanumerici.

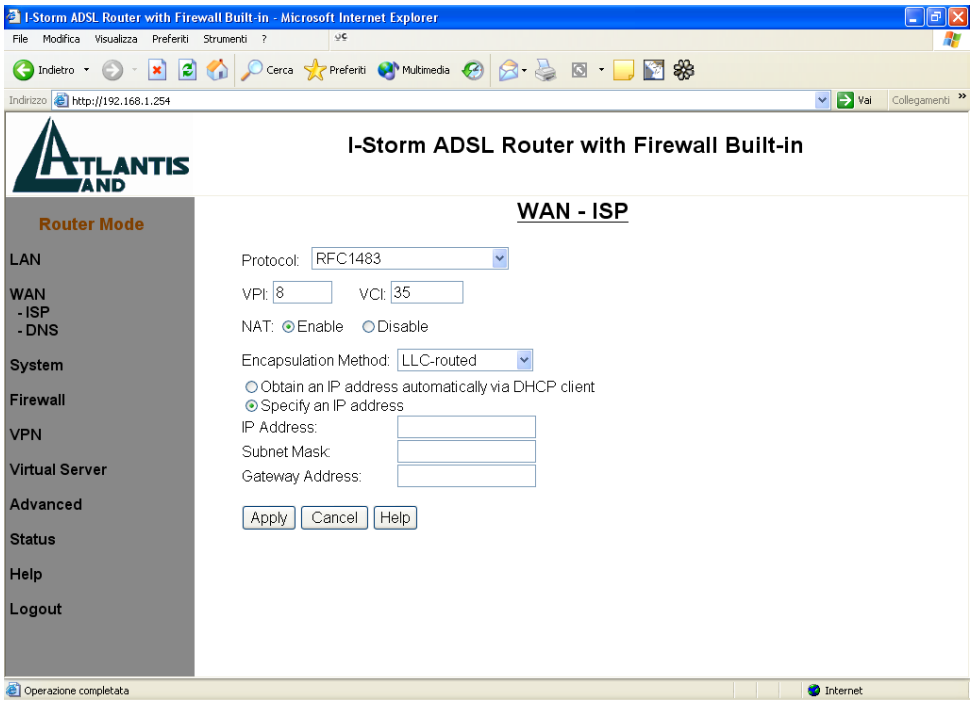
Service Name: E' un identificativo, può essere richiesto da alcuni ISP (che provvederanno a informarvi). Al solito può essere composto da massimo 63 caratteri (case sensitive) alfanumerici.

⊙ **Always On:** Scegliere questa opzione se si desidera stabilire una sessione PPPoA nel momento dello starting up. Inoltre viene automaticamente ristabilita la connessione PPPoA qualora si venga disconnessi dall'ISP (o per ragioni tecniche la connessione cada).

⊙ **Connect on Demand:** Scegliere questa opzione se si vuole stabilire una connessione PPPoA solo quando ci sono pacchetti diretti verso Internet.

Auto-disconnect if idle for more than ☐ minutes: Disconnette automaticamente il Router ADSL quando non rileva alcuna attività di pacchetti verso Internet per un tempo predeterminato. Il valore può essere settato da 0 a 999, come default è 5.

RFC1483



Configurare l'interfaccia WAN con l'IP statico (non necessariamente pubblico) assegnato dall'ISP.

NAT: Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità deve essere disabilitata.

IP Address: Introdurre l'IP statico (non necessariamente pubblico) assegnatovi dall'ISP.

Subnet Mask: Introdurre la Subnet Mask fornita dall'ISP.

Gateway Address: Introdurre l'indirizzo IP fornitovi dall'ISP che è il gateway del vostro Router ADSL.

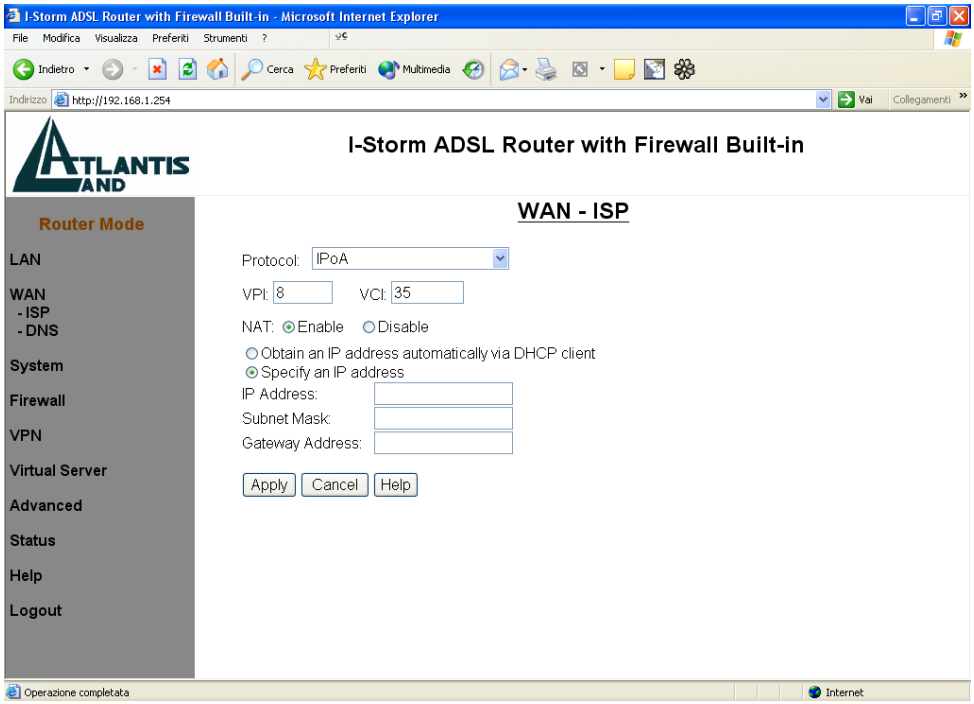
Le principali modalità in cui l'ISP può fornire RFC1483 possono essere diverse:

1-**Un indirizzo IP pubblico statico**. In questo caso bisognerà settare la sezione WAN-ISP nella seguente modalità: NAT=abilitato, IP address=IP statico pubblico assegnatovi, Subnet mask e Default Gateway (che sarà un IP pubblico) vi saranno fornite dal provider. Il LAN-IP è invece in una classe privata e sarà il default gateway di tutti i PC (se non si attiva il DHCP).

2-**Una classe di IP statici con Punto-Punto pubblica**. In questo caso bisognerà settare la sezione WAN-ISP nella seguente modalità: Nat=disabilitato, IP address=IP statico pubblico assegnatovi (quello della punto-punto) Subnet mask e Default Gateway (che sarà un IP pubblico) vi saranno fornite dal provider. Il Lan IP invece è sempre un IP statico pubblico e fa parte della classe assegnatavi con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere messi sui PC assieme al default gateway che sarà il LAN-IP (ed i DNS).

3-**Una classe di IP statici con Punto-Punto privata**. In questo caso bisognerà settare la sezione WAN-ISP nella seguente modalità: Nat=disabilitato, IP address=IP privato assegnatovi (quello della punto-punto) Subnet mask e Default Gateway (che sarà un IP privato) vi saranno fornite dal provider. Il Lan IP invece è sempre un IP statico pubblico e fa parte della classe assegnatavi con la rispettiva subnet mask. Gli altri IP di questa classe (e la subnet mask) dovranno essere messi sui PC assieme al default gateway che sarà il LAN-IP (ed i DNS).

IPoA



Configurare l'interfaccia WAN con l'IP pubblico statico assegnato dall'ISP.

NAT: Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata.

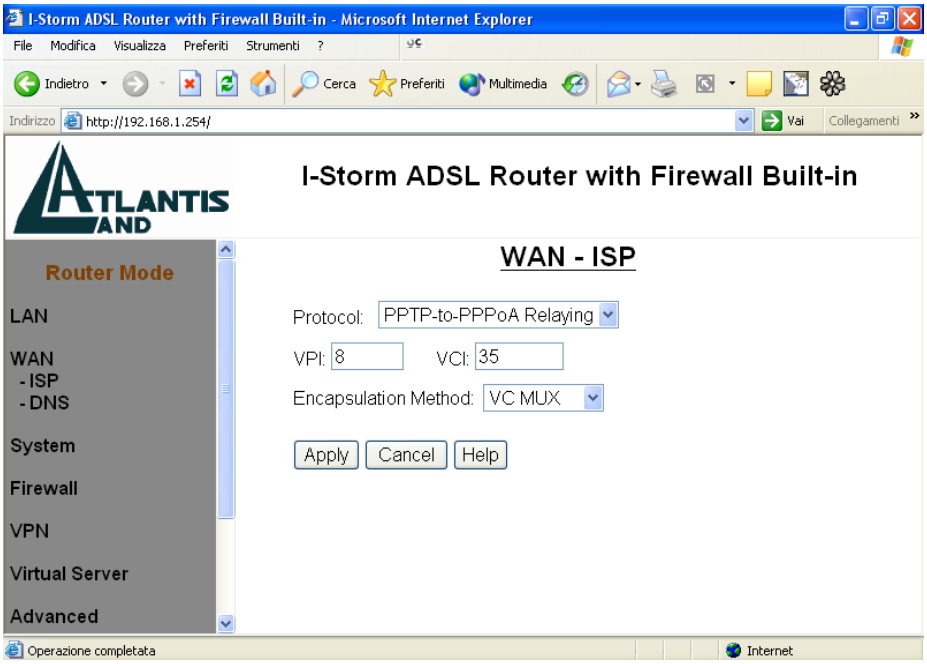
IP Address: Introdurre l'IP pubblico statico assegnatovi dall'ISP.

Subnet Mask: Introdurre la Subnet Mask fornita dall'ISP.

Gateway Address: Introdurre l'indirizzo IP fornitovi dall'ISP che è il gateway del vostro Router ADSL.

Per ulteriori dettagli consultare la sezione precedente (RFC1483).

PPTP-to-PPPoA Relaying

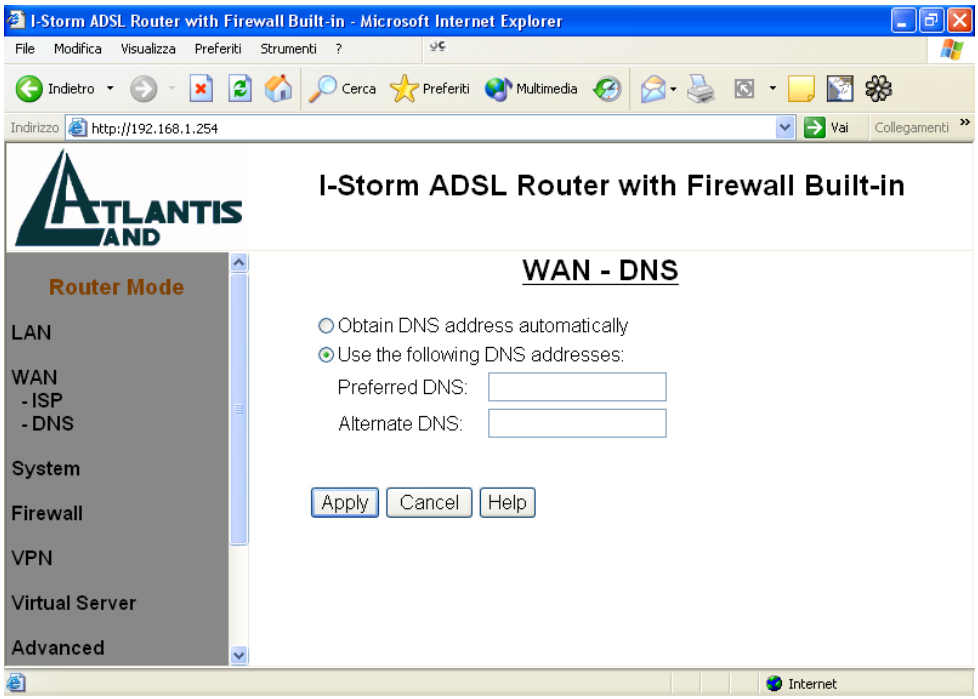


Può essere usata per stabilire un tunnel PPTP tra il client PPTP sulla Lan ed il Router. IL Router si occuperà della gestione e conversione dei pacchetti PPTP verso/da pacchetti PPP. Il Router stabilisce una connessione PPPoA con l'ISP. E' necessario, per terminare, creare un acceso di tipo VPN dal PC indicando l'indirizzo IP quello LAN IP del Router ed inserendo username e password dati dall'ISP. In questa modalità l'indirizzo IP assegnato al Router viene ruotato al PC che pertanto ha un IP pubblico, ciò può essere utile per ottenere il pieno funzionamento di alcune particolari applicazioni internet. **Ovviamente un solo PC alla volta può usare l'accesso ad Internet**. Per ulteriori dettagli, su come costruire la VPN, consultare la sezione 3.5.2.

DNS

Un Domain Name System (DNS) contiene una tabella di corrispondenze tra nomi di domini ed indirizzi IP pubblici. In Internet un certo sito ha un unico nome come www.yahoo.com ed un indirizzo IP. L'indirizzo IP è difficile da ricordare (però è assolutamente il modo più efficiente), certamente molto più del nome. Questo compito è svolto appunto dal DNS che grazie alla tabella incorporata riesce a fornire al PC che ne fa richiesta l'indirizzo IP corrispondente al nome del sito (e qualora non l'avesse la richiederà ad altri server DNS di cui conosce l'IP). Gli indirizzi IP dei DNS sono forniti dall'ISP al momento in cui si effettua il LogOn. Selezionando **Obtain DNS address automatically** (di default con PPPoE e PPPoA) si ottengono questi indirizzi in maniera automatica. Se il protocollo è

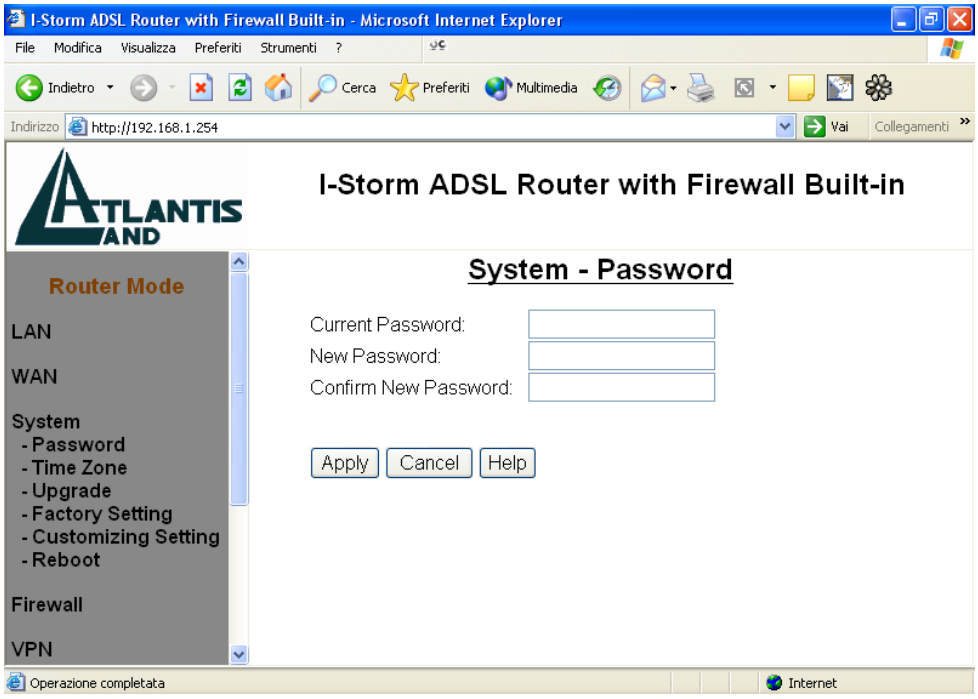
RFC 1483, IpoA o PPTP-to-PPPoA Relaying è necessario introdurre manualmente gli indirizzi IP dei DNS dell'ISP.



Scegliendo infatti uno dei protocolli RFC1483, IpoA o PPTP-to-PPPoA Relaying nella sezione ISP apparirà la maschera di sopra. Bisogna introdurre gli indirizzi IP dei DNS che vi saranno forniti dall'ISP. E' necessario inoltre mettere tali valori dei DNS in ogni PC della Lan.

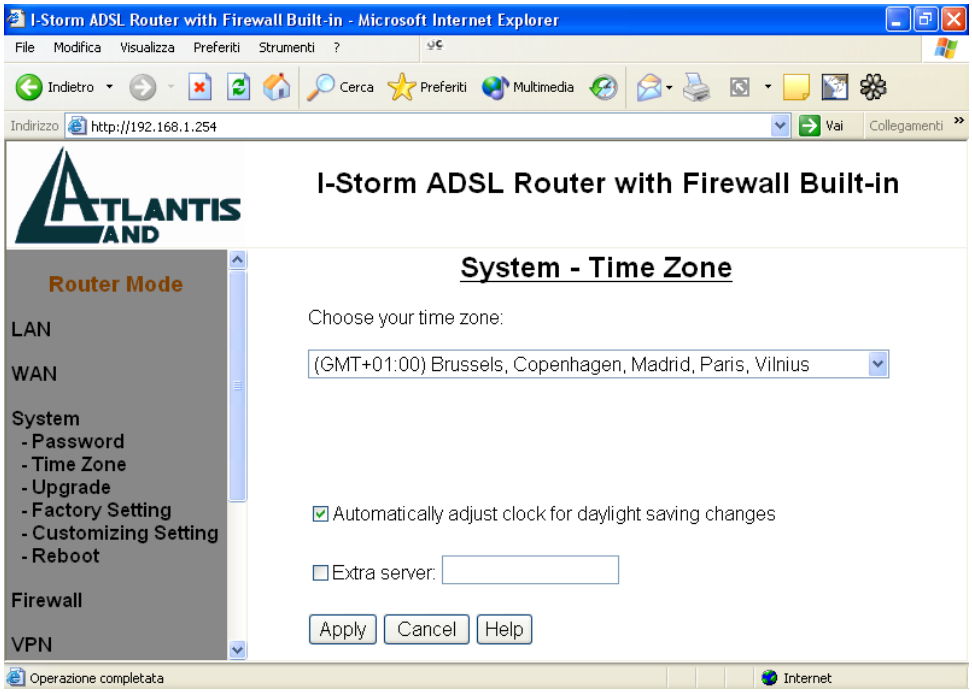
3.4.3 System

Password



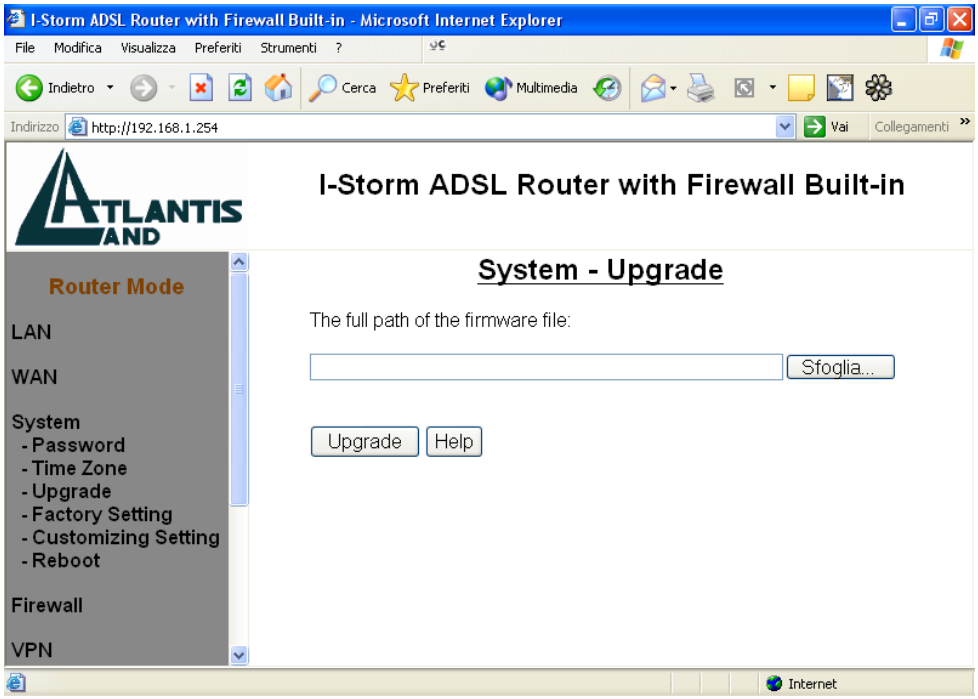
Le impostazioni di default non comprendono alcuna password. E' consigliabile cambiare tale settaggio al fine di evitare spiacevoli intrusioni. E' necessario conservare la nuova password in un posto sicuro, in quanto **non è possibile in alcun modo** (se non rivolgendosi ad AtlantisLand spa ed avendo **l'indirizzo MAC del Router**) **accedere al Router (via web)ADSL qualora venga persa**. La password può essere lunga sino ad 8 caratteri alfanumerici (accertarsi che la posizione del Caps Lock sia off). Nell'ipotesi si perdesse la password fare riferimento alla sezione opportuna contenuta nel capitolo 4.

Time Zone



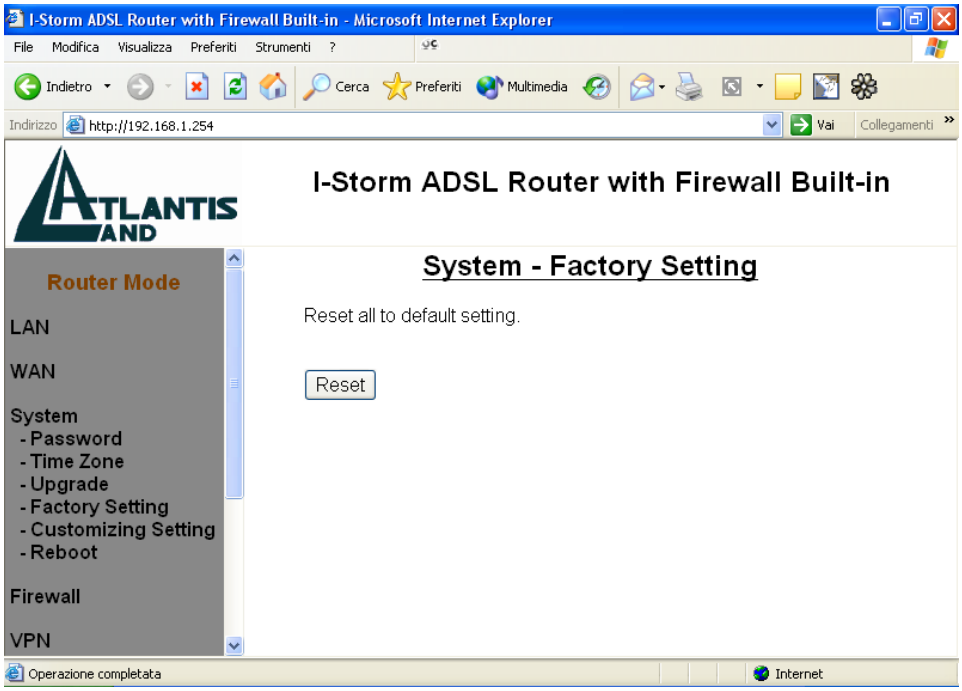
Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente. Per scegliere la zona di appartenenza sarà sufficiente accedere, sotto il menù **System** nel Menù principale, alla voce **Time Zone** e poi, una volta scelto il fuso di appropriato, premere poi il tasto **Apply**. E' possibile ricevere, pertanto, l'ora corretta solo dopo che il collegamento ad Internet è effettivo. E' possibile controllare l'ora segnata dal Router ADSL accedendo, sotto il menù **Status** nel Menù principale, alla voce **System Status** (cliccare sul tasto **Refresh** per aggiornare la tabella mostrata).

Upgrade



Per effettuare l'upgrade del firmware del Router ADSL è necessario anzitutto scaricare dal sito www.atlantisland.it o www.atlantis-land.com (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù **System** nel Menù principale, alla voce **Upgrade** e premere poi il tasto **Sfoglia** ed indicare la path dove si è messo il file del firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. **E' opportuno non staccare, durante la fase di upgrade, il Router ADSL dalla presa elettrica**. Completata la procedura il RouterADSL si resetterà automaticamente e inizierà a funzionare col nuovo firmware. Tutti i settaggi precedenti del Router ADSL dovrebbero essere conservati.

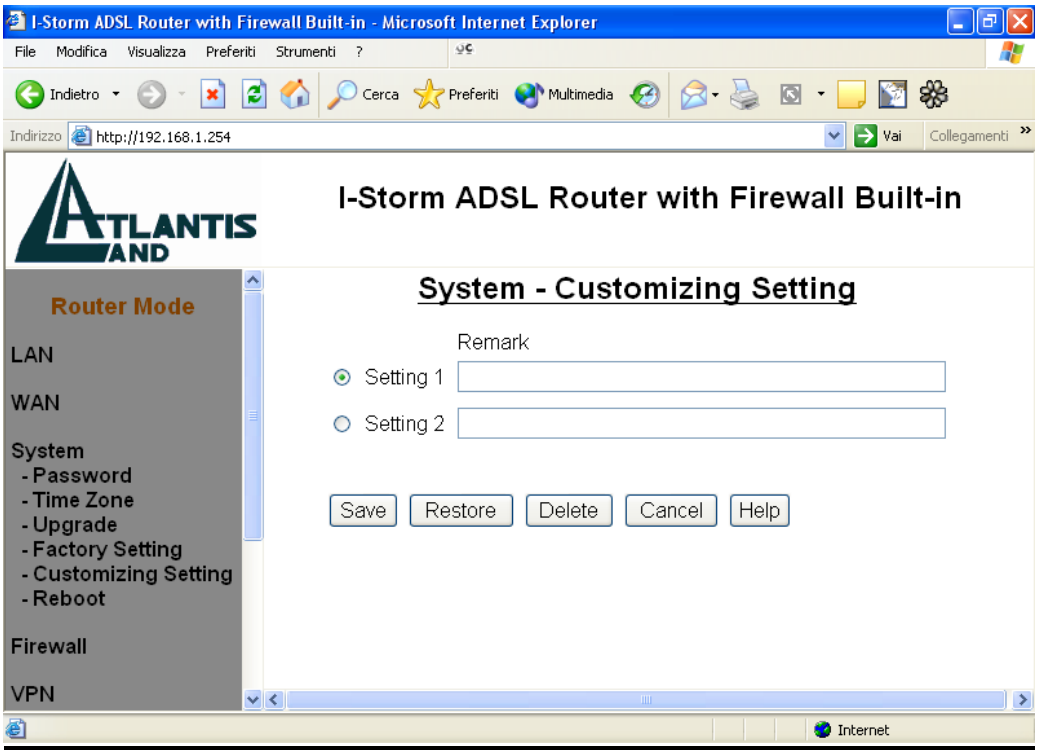
Factory Setting



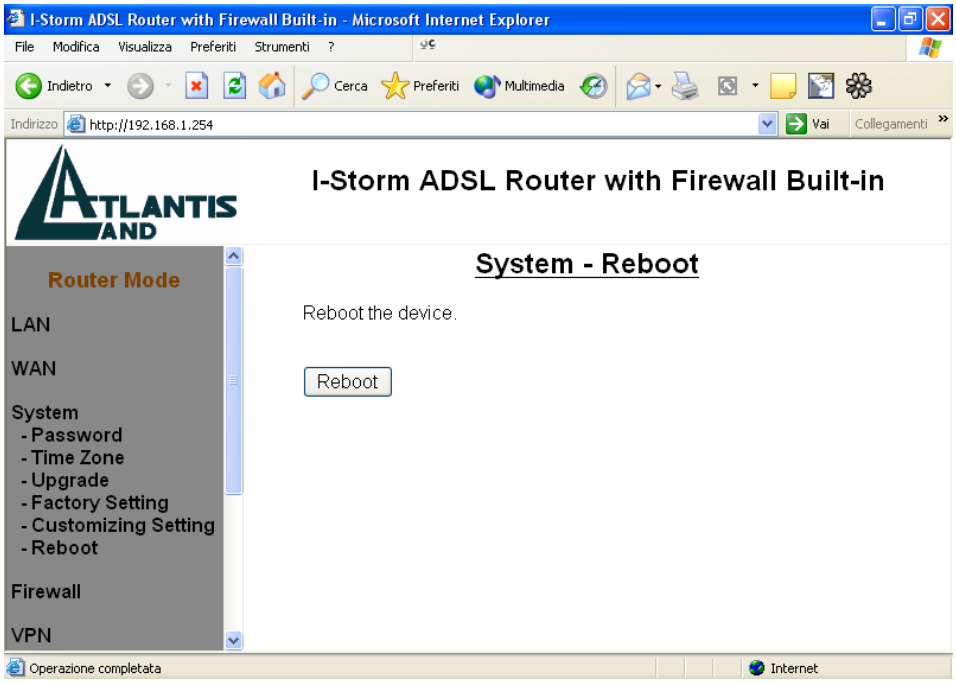
Se per necessità si desidera reimpostare il router ADSL con la configurazione di default (perdendo tutti i settaggi inseriti) sarà sufficiente accedere, sotto il menù **System** nel Menù principale, alla voce **Factory Setting** e premere poi il tasto **Reset.** I valori della configurazione di default sono riportati nella sezione 3.2 di questo manuale.

Customizing Setting

L'I-Storm ADSL Router consente di memorizzare due configurazioni diverse, allo stesso tempo. Sarà sufficiente salvare le singole configurazioni, mettendo nel campo Remark un nome che ci aiuterà nel ricordare il tipo di configurazione. A questo punto premere sul tasto Save per salvare la configurazione col nome inserito. Sarà sufficiente per ripristinarla, in un secondo momento, evidenziarla (col bottone sulla sinistra) e poi premere il tasto Restore.



Reboot



Qualora il dispositivo smetta di rispondere o funzionare è possibile risolvere il problema accedendo, sotto il menù **System** nel Menù principale, e cliccare la voce **Reboot.** Apparirà la finestra sottostante in cui un timer vi aggiornerà sul tempo necessario alla riconnessione.

3.4.4 Firewall

Questa funzionalità offerta dal Router ADSL è un firewall che consente una prima valida difesa nei confronti di qualche malintenzionato di cui Internet è piena. Come già detto le funzionalità offerte, pur essendo varie ed efficaci, non sono da ritenersi "sicure" sempre e comunque. Certamente potrebbero essere considerate ampiamente soddisfacenti in molte circostanze, ma la varietà degli attacchi e la velocità con cui Internet si evolve consiglia sempre di non considerarsi inattaccabili. Qualora le informazioni custodite siano particolarmente importanti consigliamo un'attenta configurazione del firewall e magari l'uso di prodotti, a supporto, più adatti al caso.

Un utente può decidere di abilitare il firewall del Router composto sostanzialmente dalle seguenti sottosezioni: **Packet Filter, Block Hacker Attack e Block WAN**. Le prestazioni possono decrescere dal 5% sino al 10% a seconda del tipo di controlli che si richiedono al firewall. E' consigliabile visitare periodicamente il sito di AtlantisLand (www.atlantisland.it o www.atlantis-land.com) al fine di reperire l'ultimo Firmware che potrebbe migliorare le caratteristiche del firewall.

Packet Filter

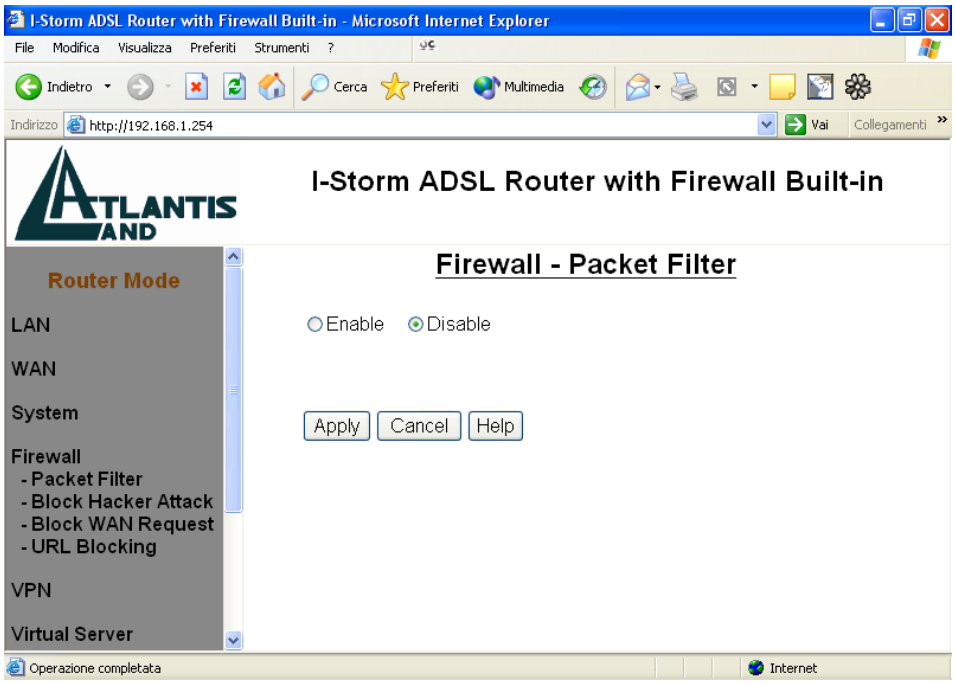
Queste funzioni di filtraggio dei pacchetti IP sono in buona sostanza una serie di regole che il Router ADSL applicherà ai pacchetti IP che lo attraversano e stabilirà o meno il soddisfacimento di queste regole, pacchetto per pacchetto. E' utile comunque sapere che il solo filtraggio sui pacchetti non elimina i problemi legati a livello di applicazioni o altri livelli.
Le politiche con cui organizzare un filtraggio sono essenzialmente riassumibili in **due posizioni**:
Blocco ciò che conosco come pericoloso e consento il passaggio del resto: Tale posizione dovrebbe essere applicata da coloro che possiedono una discreta conoscenza di Internet. Richiede la conoscenza dei pericoli da filtrare opportunamente e consente, nella maggior parte dei casi, di non imbattersi in decine di applicazioni che hanno problemi perché mal configurate (con questo filosofia si blocca solo il pericolo). In questo caso bisognerà formare un nuovo set di regole (vedere sotto) scegliendo come azione il **drop**.

Passa solo quello che ritengo sicuro il resto è bloccato: Tale posizione dovrebbe essere applicata da coloro che possiedono una buona conoscenza di Internet in quanto è necessario predisporre una regola per ogni "servizio" che si vuole usare. E' certamente più sicura ma richiede una maggiore conoscenza delle problematiche ed una più lunga preparazione delle regole dei filtri (che possono essere moltissimi). In questo caso bisognerà formare un nuovo set di regole (vedere sotto) scegliendo come azione il **forward**.
E' opportuno fare una regola finale che tagli tutto (Active=yes, Packet Type=Any, Action=Drop,). In questo modo tutti i pacchetti entranti che non sono stati già inoltrati vengono eliminati rispettando la filosofia generale di questo approccio.
Qualora si usasse il NAT, e dunque nessun PC della Lan ha in dotazione un IP pubblico, la rete dovrebbe essere già sufficientemente protetta in ingresso.

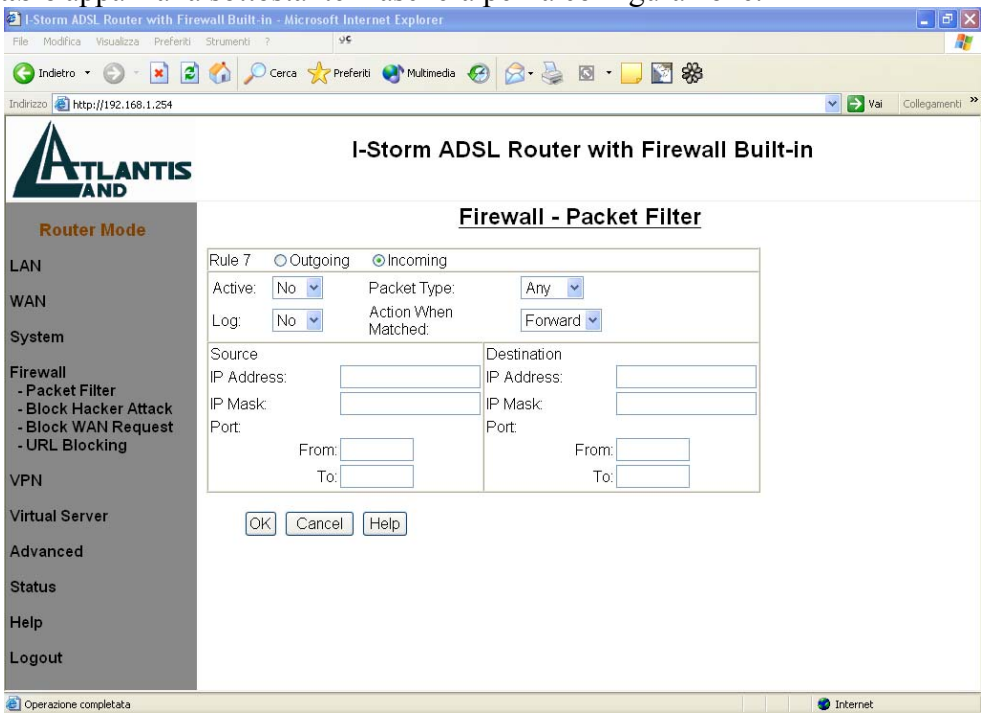
Una volta realizzate le regole che determinano il modo in cui avviene il filtraggio dei pacchetti IP è opportuno **verificare la sicurezza del sistema**. Questo è realizzabile in diverse modalità:

1-Sito specializzato: In questo caso è possibile ottenere un primo risultato visitando il sito **http://www.dslreports.com** (ve ne sono ovviamente moltissimi altri) e accedendo alla sezione DSLR Tools ed infine scegliere Port-Scan. I risultati possibili, per ogni porta controllata, possono essere 3 (**open:**la porta è in ascolto e dietro c'è un servizio che accetta le connessioni, **closed:**la porta rifiuta la connessione e non è dato sapere se c'è un servizio dietro, **stealth:** la porta non risponde alla richiesta di connessione)

2-PC esterno alla vostra LAN: In questo modo potete provare i vostri filtri**.**



La funzionalità di Packet filtering consente di configurare il Router ADSL per bloccare da e per Internet specifici indirizzi IP (esterni o interni) o specifiche porte e dunque servizi a queste associate. Scegliendo **Enable** apparirà la sottostante maschera per la configurazione.



E' possibile configurare sino a 20 regole (col firmware V2.2.4) che permettono un adeguato controllo di quello che attraversa il Router ADSL. La relazione logica tra le regole e di tipo **OR** , il Firewall testa il pacchetto che lo attraversa, a partire dalla regola numero 1. Non appena una regola è

soddisfatta viene eseguita l'azione specifica, ed il pacchetto NON viene esaminato dalle regole successive.

Add: Cliccare su questo bottone per aggiungere una nuova regola. Dopo il click apparirà la maschera sottostante.

Edit: Scegliere il numero di regola che si vuole modificare e cliccare poi sul bottone EDIT per modificarla. Apparirà comunque la maschera sottostante.

Delete: Scegliere il numero di regola che si vuole modificare e cliccare poi sul bottone DELETE per cancellarla.

Move Up/Move Down: Scegliere il numero di regola che si vuole alterare. Cliccare dunque sul bottone "Move Up" oppure "Move Down" per cambiarne la sequenza. La posizione delle regole è importante, a titolo d'esempio si potrebbe pensare (vedere l'**esempio 1**) di mettere prima la regola che consenta il passaggio dell'UDP 53 (quella per richiedere l'indirizzo IP dell'URL digitato al DNS) rispetto a quella del TCP 80 (il normale http). In effetti il primo pacchetto uscente sarebbe quello indirizzato al DNS e la regola funzionerebbe bene risparmiando qualche confronto, ma dopo che si è venuti a sapere l'IP dal server DNS, TUTTI i pacchetti (che saranno TCP 80) saranno esaminati dalla regola UDP 53 e solo dopo da quella TCP 80, facendo quindi un confronto in più (per ogni pacchetto). Un'attenta analisi del tipo di traffico può portare ad un ordine delle regole non banale ma ottimizzato per l'uso.

⊙ **Outgoing** ⊙ **Incoming:** Determina su quale tipo di pacchetti la regola va applicata, se i pacchetti uscenti o entranti.

Active: Scegliere "Yes" per abilitare la regola, oppure scegliere "No" per disabilitare la regola..

Packet Type: Specificare il tipo di pacchetto cui la regola sarà applicata(TCP, UDP, ICMP oppure any).

ICMP (Internet Control Message Protocol) Viene usato per notificare al mittente eventuali problemi legati ai datagrammi IP. I principali messaggi dell'ICMP sono: **Destination Unreachable** (l'host non è raggiungibile e pertanto il pacchetto non sarà consegnato), **Echo Reply ed Echo Request** (usati per verificare la raggiungibilità di alcuni host nella rete), **Parameter Problem** (indica che un Router che ha esaminato il pacchetto ha rilevato un qualche problema nell'intestazione), **Redirect** (usato da un host o un Router per avvisare il mittente che i pacchetti dovrebbero essere inviati ad un altro indirizzo), **Source Quench** (inviato da un Router congestionato al mittente per informarlo dello stato), **Timestamp e Timestamp Reply** (simili ai messaggi di Echo, ma aggiungono l'orario) **TTL Exceeded** (il campo TTL è sceso a zero, dunque il pacchetto è stato scartato e ne viene informato il mittente).

TCP (Transmission Control Protocol) Tale protocollo fornisce un servizio di comunicazione basato sulla connessione (al contrario dell'IP e UDP). Tale servizio è affidabile. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). E' usato moltissimo specie per Telnet (porta 23), FTP (porta 20 e 21), http (porta 80), SMTP e POP3 (porta 25 e 110).

UDP (User Datagram Protocol) Tale protocollo fornisce un servizio di comunicazione non basato sulla connessione (come dell'IP). Tale servizio è più veloce del TCP sebbene meno sicuro. Vengono utilizzate le porte di origine e destinazione (interi di 16 bit). E' utilizzato per interrogare i DNS.

Log: Scegliere "Yes" se si desidera generare un file logs quando la regola è applicata ad un pacchetto in transito sul Router ADSL. Questo file è consultabile accedendo alla sezione **Status** e poi **Security Log**.

Action When Matched: Quando un pacchetto soddisfa la regola, bisogna dire se eliminare (**drop**) o far passare il pacchetto in questione (**forward**).

Source IP Address: Introdurre l'indirizzo IP sorgente dei pacchetti (che possono essere entranti o meno).

Source IP Mask: Introdurre la Subnet Mask sorgente dei pacchetti.

Source Port: Numero di porta sorgente da controllare per TCP o UDP.

Destination IP Address: : Introdurre l'indirizzo IP destinatario dei pacchetti (che possono essere entranti o meno).

Destination IP Mask: Introdurre la Subnet Mask degli IP di destinazione dei pacchetti.

Destination Port: Numero di porta di destinazione da controllare per TCP o UDP

Bisogna prestare particolare attenzione alle porte in funzione della tipologia di pacchetti (entranti o uscenti). Se si desidera filtrare l'http è possibile farlo impostando un filtro tanto per i pacchetti entranti che per quelli uscenti. Se il filtro è applicato ai pacchetti uscenti bisognerà selezionare come porta di destinazione (Destination) la 80. Se il filtro invece è applicato ai pacchetti entranti la porta di provenienza (Source) sarà la 80. Per ulteriore documentazione si faccia riferimento ad una guida sull'uso delle porte nel TCP/IP.

Qualora nelle regoledel firewall si scegliesse di filtrare, come protocollo, ICMP o ANY, non sono disponibili (non facendone uso questi protocolli) le porte.

Vediamo adesso in pratica questi concetti tramite un paio di esempi:

Esempio 1

Costruiremo adesso una serie di regole utilizzando un approccio di tipo conservativo, faremo cioè entrare solo quello che riterremo sicuro (usando il NAT nessuna chiamata originata dall'esterno sarebbe passata, ma si potrebbe desiderare che nessuna applicazioni comunque passi per determinate porte), con una serie di regole, e limiteremo tutto il resto del traffico in ingresso con una regola finale.

Filtro **Passa FTP**. Faremo una nuova regola con le seguenti caratteristiche evidenziate: Incoming, Active=Yes, Log=Yes, Racket Type=TCP, Action When Matched=Forward, lasceremo vuoti i campi Source IP e Destination IP per non ledere in generalità, Source Port From=20 e Source Port to=21, Destination Port From=0, Destination Port to=65535. In questo modo ogni richiesta entrante sulla porta 20 e 21 sarà inoltrata. Qualora non dovesse funzionare è possibile nel browser la modalità passiva (strumenti-opzioni internet-avanzate e selezionare la voce **usa un FTP passivo**).

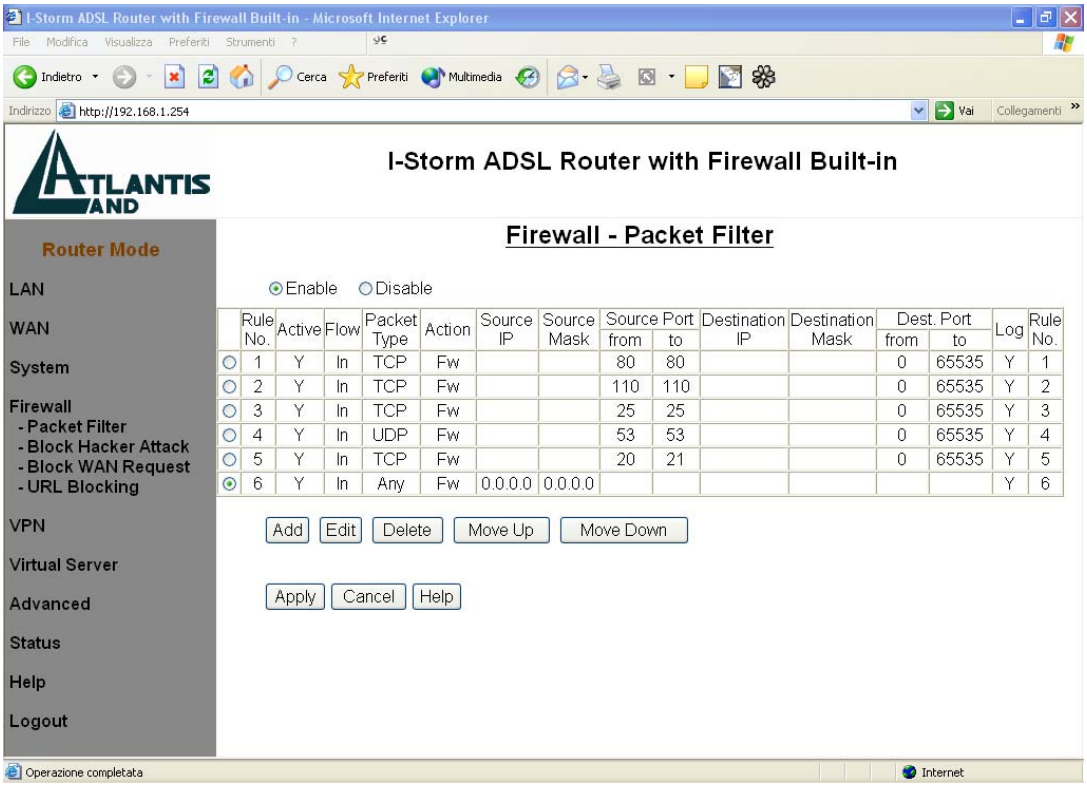
Filtro **Passa HTTP.** Faremo una nuove regola con le seguenti caratteristiche evidenziate: Incoming, Active=Yes, Log=Yes, Racket Type=TCP, Action When Matched=Forward, lasceremo vuoti i campi Source IP e Destination IP per non ledere in generalità, Source Port From=80 e Source Port to=80, Destination Port From=0, Destination Port to=65535. In questo modo ogni pacchetto entrante sulla porta 80 sarà inoltrato.

Filtro **Passa DNS**. Faremo inoltre una regola che consente il passaggio dell'UDP 53, per la risoluzione dei DNS. Incoming, Active=Yes, Log=Yes, Racket Type=UDP, Action When Matched=Forward, lasceremo vuoti i campi Source IP e Destination IP per non ledere in generalità, Source Port From=53 e Source Port to=53, Destination Port From=0, Destination Port to=65535. Si potrebbe essere più precisi limitando anche l'IP di provenienza a quelli dei DNS (ma presenta degli svantaggi). In questo modo, con le 2 regole (Passa DNS e Passa http), riusciremo a usare i server DNS e vedere i siti http.

Alla stessa maniera creeremo 2 regole per il passaggio della posta (TCP 25 e TCP 110) ed eventualmente altre per servizi diversi.

Regola **Finale**. Faremo una nuove regola con le seguenti caratteristiche evidenziate: Incoming, Active=Yes, Log=Yes, Racket Type=any (potremmo scegliere TCP), Action When Matched=Drop, lasceremo campi Source IP= **0.0.0.0**, subnet =**0.0.0.0** e vuoti gli altri. per non ledere in generalità. In questo modo ogni pacchetto, che non sia già stato inoltrato dalle regole precedenti, e che dunque vuole parlare con una porta diversa da quelle concesse viene eliminato. In tal modo eventuali Trojan non riusciranno ad essere facilmente controllati dall'esterno ed aumenteremo la sicurezza della Lan.

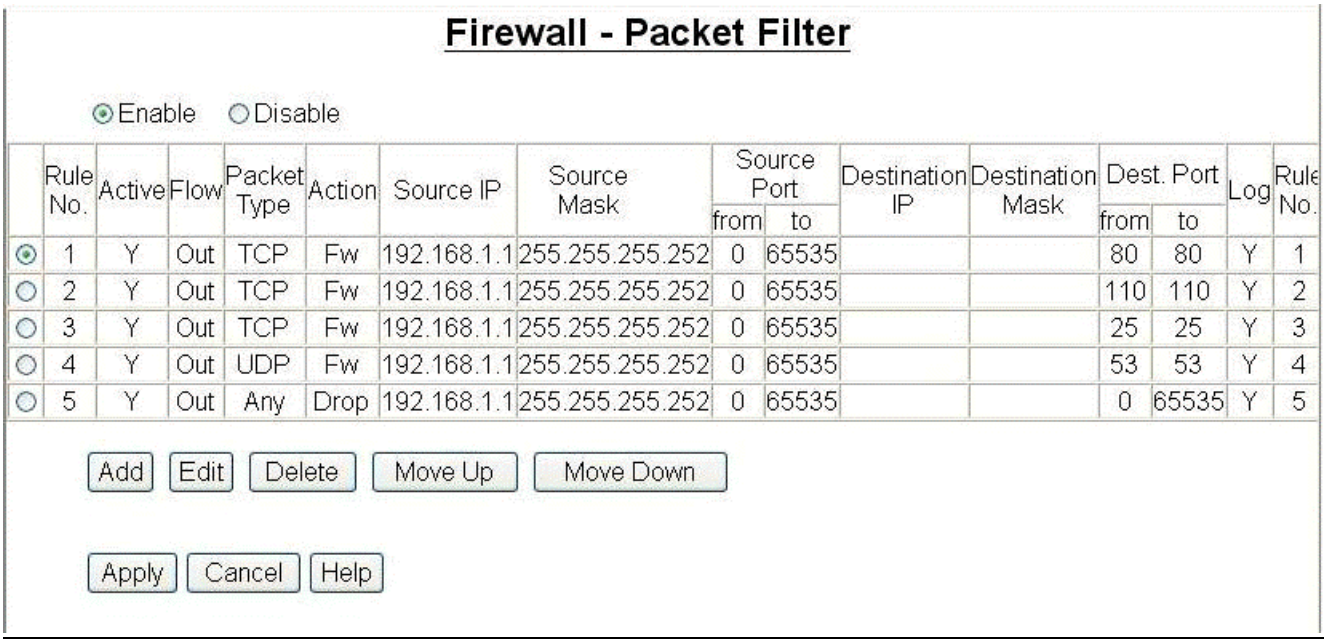
*La regola **Finale** non deve essere assolutamente spostata di ordine**,** se così fosse tutte le regole che la seguirebbero non sarebbero mai applicate poiché nessun pacchetto sarebbe loro passato.*



Dovreste ottenere un'immagine del genere.

Esempio 2

Anzitutto è necessario assegnare ai PC che si vogliono limitare degli indirizzi IP fissi e disabilitare così, qualora fosse attivo, il client DHCP. In questo modo, avendo sempre i medesimi indirizzi IP potremo operare correttamente (si ricorda che invece se fossero client DHCP l'indirizzo IP potrebbe mutare). L'idea da seguire sono le seguenti: **Utenti appartenenti al gruppo A** saranno filtrati ed **Utenti appartenenti al gruppo B** avranno invece accesso senza alcuna limitazione a tutti i servizi internet. Per ottenere questo creeremo nel firewall dell'I-Storm tutta una serie di regole che consentiranno il passaggio per i pacchetti uscenti e provenienti dagli IP dei PC del gruppo A dei vari servizi consentiti. Creeremo poi una regola finale che eliminira tutti i pacchetti uscenti provenienti dagli IP dei PC del gruppo A (saranno quei pacchetti che non sono passati nelle regole di sopra e che dunque non sono autorizzati ad uscire). Vediamo adesso come scegliere gli IP del gruppo A. Anzitutto saranno IP contigui (appartenente alla classe 192.168.1.x per esempio). Creiamo la regola 1 per pacchetti uscenti che se soddisfatta inoltra il pacchetto (qualora un pacchetto non la soddisfa si passa alla regola 2 e così via). Tale regola deve consentire la visione delle pagine WEB. Metteremo nel campo Source l'indirizzo IP di un PC del gruppo A, poi come subnet metteremo 255.255.255.252 (per 4 elementi, oppure 248 per 8 elementi). Sceglieremo TCP, come azione Forward e come porta di destinazione la 80. Faremo poi le regole che consentono il passaggio delle porte TCP 110 e TCP 25 (entrambe per la posta) ed UDP 53 per la risoluzione dei DNS. Fatto questo faremo la regola finale che taglia tutti i pacchetti provenienti da questi IP che non hanno passato nessuna regola antecedente, questa regola avrà come azione Drop. Dovrebbe apparire un risultato analogo alla foto di sotto:



Firewall - Packet Filter

◉ Enable ○ Disable

	Rule No.	Active	Flow	Packet Type	Action	Source IP	Source Mask	Source Port		Destination IP	Destination Mask	Dest. Port		Log	Rule No.
								from	to			from	to		
◉	1	Y	Out	TCP	Fw	192.168.1.1	255.255.255.252	0	65535			80	80	Y	1
○	2	Y	Out	TCP	Fw	192.168.1.1	255.255.255.252	0	65535			110	110	Y	2
○	3	Y	Out	TCP	Fw	192.168.1.1	255.255.255.252	0	65535			25	25	Y	3
○	4	Y	Out	UDP	Fw	192.168.1.1	255.255.255.252	0	65535			53	53	Y	4
○	5	Y	Out	Any	Drop	192.168.1.1	255.255.255.252	0	65535			0	65535	Y	5

Add Edit Delete Move Up Move Down

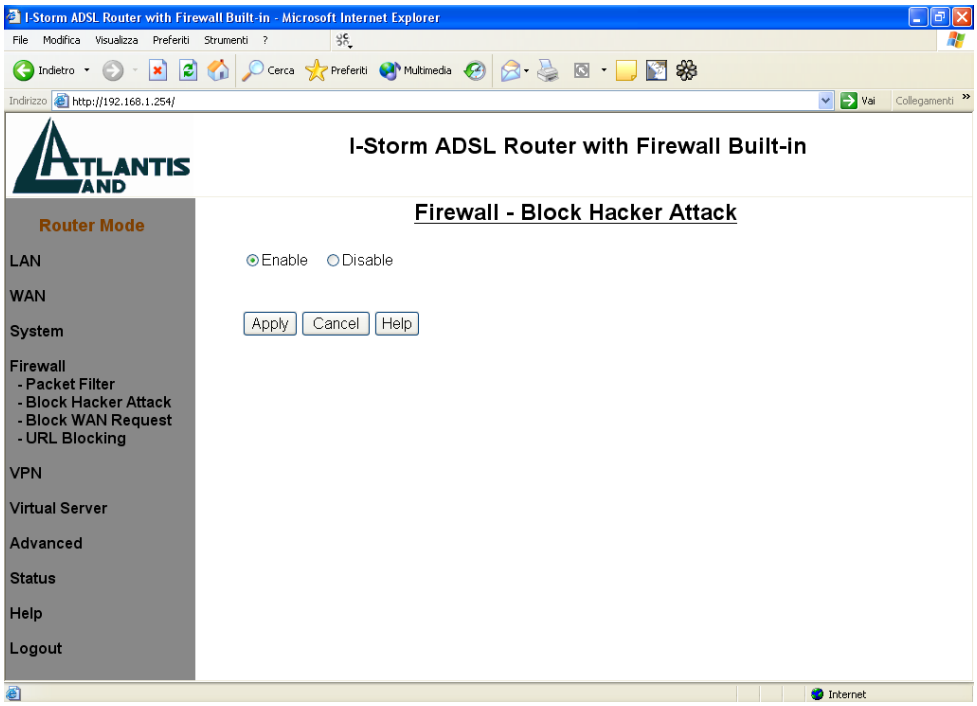
Apply Cancel Help

In questo modo i pacchetti uscenti appartenenti al gruppo A e che soddisfano le regole sono inoltrati, quelli provenienti da A e che non soddisfano le regole di inoltro sono eliminati dalla regola 5. I pacchetti provenienti da altri IP sono semplicemente inoltrati perchè non soddisfano alcuna regola. E' possibile creare più gruppi e per ogni gruppo consentire determinati servizi.

Scelta dei gruppi. E' opportuno per evitare errori scrivere gli indirizzi IP in binario così come la subnet mask. Facciamo un esempio:**44** in binario diviene **00101100.** La subnet mask 248 è 11111000. Quindi mettere come IP=192.168.168.44 e subnet mask=255.255.255.248 significa indicare in binario tutti quegli IP che cambiano i soli ultimi 3 bit (000,001....111). Cioè da 192.168.1.40 sino

192.168.1.47. Se avessimo usato come subnet 252 (11111100) avremmo potuto cambiare solo gli ultimi 2 bit pertano avremmo avuto da 192.168.1.44 a 192.168.1.47. Resta inteso che i gruppi, per via delle subnet, sono solo nei seguenti multipli:2,4,8,16,32,64,128 o 255. Nel caso, ad esempio, con 3 utenti si può mettere 192.168.1.1 e mettere subnet 255.255.255.252 in questo modo si settano i primi 4 (192.168.1.1, 192.168.1.2, 192.168.1.3) oppure mettendo 255.255.255.248 si arriva sino al 192.168.1.7. Tutti gli altri IP (sino 253) non saranno filtrati e potranno essere assegnati ai PC che non hanno limitazioni.

Block Hacker Attack



Il Router può automaticamente accorgersi e bloccare un attacco di tipo DoS (Denial of Service) se questa funzione è attiva. Lo scopo di attacchi di questo tipo non è quello di cogliere informazioni particolari dalla vostra rete quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Più precisamente esistono 4 specifici tipologie di attacchi DoS.

1-Attacchi che mirano all'esaurimento della banda, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente, altrimenti può usare altri host che di fatto amplificano l'attacco.

2-Attacchi che mirano all'esaurimento delle risorse.

3-Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware.

4-Attacchi DoS generici.

Vengono riconosciuti diversi tipi diversi di patterns tra i quali:

- **IP Spoofing**
- **Ping of Death (Length > 65535)**
- **Land Attack (Same source / destination IP address)**
- **IP with zero length**
- **Sync flooding**

- **Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)**
- **Snork Attack**
- **UDP port loop-back**
- **TCP NULL scan**
- **TCP XMAS Scan**
- **WinNuke Attack**
- **TCP SYN Flooding**
- **Ascend Kill**
- **IMAP SYN/FIN scan**
- **Net Bus scan**
- **Back Orifice scan**

Segue una breve descrizione del funzionamento degli attacchi più comuni.

IP Spoofing è un attacco particolare in cui l'attaccante cerca di intromettersi in una connessione con lo scopo di abbatterla o di prenderne il controllo. Può essere fatto sia dall'interno della propria Lan (con possibilità più alte di successo se si dispone di LAN con HUB) che da Internet con possibilità di successo infinitamente inferiori. Grazie al SPI il Router esamina a fondo i pacchetti che lo attraversano e confrontando molti parametri coi pacchetti precedenti della stessa connessione riesce a stabilire con efficacia se un pacchetto in arrivo è "spoofato" o meno.

Sync Flood, come già accennato è un attacco che mira a esaurire le risorse del sistema che lo subisce. All'atto dell'instaurazione di una connessione viene spedito un pacchetto (dall'attaccante) col quale si avvisa che si vuole costruire la connessione. Il ricevente, cioè l'attaccato, alloca delle risorse e risponde con un pacchetto per proseguire la creazione della connessione. L'attaccato aspetta pazientemente il pacchetto di risposta (che non arriverà mai poiché l'attaccante avrà scelto o un IP di un host spento oppure starà attaccando l'host in questione impedendogli di rispondere). Le risorse allocate saranno bloccate sino a che non scade il timer associato. Nel frattempo l'attaccante ripeterà quest'attacco finendo col bloccare tutte le risorse disponibili nell'attaccato. Il firewall integrato nell'I-Storm ADSL Router riconosce il tentativo di apertura di diverse connessioni provenienti dallo stesso IP e non allocherà le risorse. Certamente, a meno di trovarsi con sprovveduti, l'IP che verrà registrato nella tabella del sicurity logs non apparterrà all'attaccante.

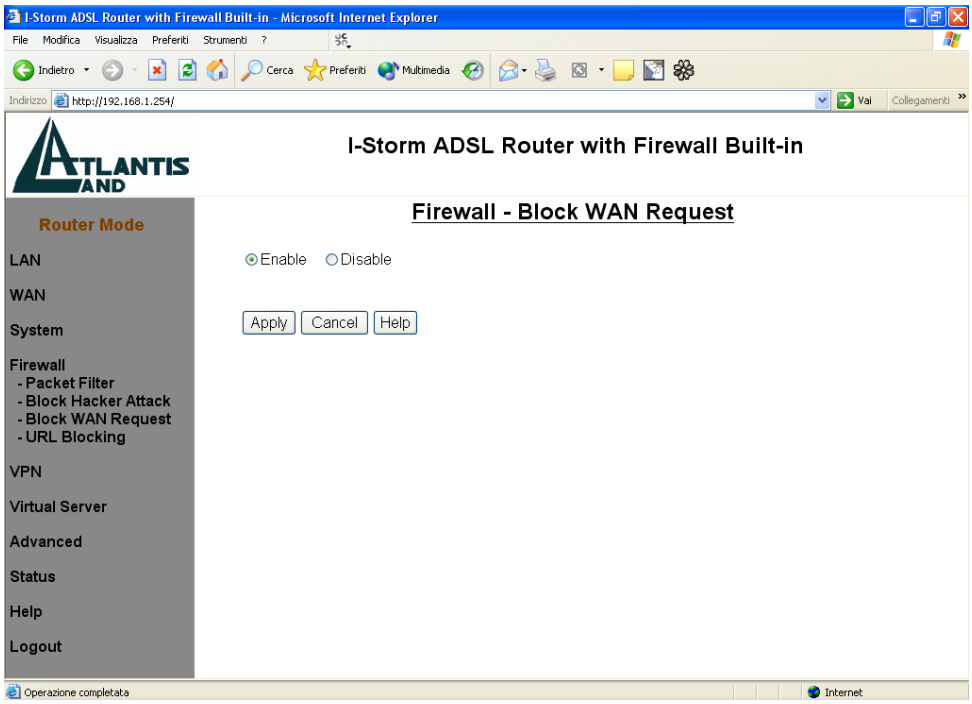
Smurf Attack, tenta invece di esaurire l'intera banda dell'host vittima, per fare questo può (a seconda della velocità della sua connessione) sfruttare anche delle sottoreti che fungono da amplificatore. Infatti l'indirizzo di broadcast di queste sottoreti vieni sfruttato e così tutti gli host di questa sottorete rispondono all'Echo Request richiesto dall'attaccante che avrà sostituito l'IP del mittente con quello dell'attaccato. All'attaccato tutti gli host risponderanno col pacchetto di Echo Reply generando un traffico intensissimo. L'I-Storm ADSL Router filtra i pacchetti di Echo Reply in uscita trattandolo come un attacco.

Ping of Death, quest'attacco particolare e dalle conseguenze variabili (anche a seconda del carico della macchina) viene generato creando un pacchetto ICMP di Echo Request fuori standard. Il pacchetto IP può infatti essere lungo, dalle spefiche RFC, al massimo 65536 bytes di cui 20 sono riservati per l'header. Entro il Payload vengono inseriti i pacchetti di livello superiore, in questo caso l'ICMP (oppure TCP, UDP) che ha un header lungo 8 bytes. La lunghezza massima per il Payload del

pacchetto ICMP è dunque 65535-20-8=60507 bytes. Sebbene un pacchetto del genere sia fuori specifica è comunque realizzabile, inoltre arriva frammentato alla destinazione (l'attaccato) dove verrà ricomposto (non verificandolo prima) ma a questo punto potrebbe generare un overflow dello stato di alcune variabili. Il firewall integrato si accorge di questo tipo di attacco e scarta il pacchetto in questione, aggiornando la tabella del security logs.

Land Attack, sfrutta un errore presente in molti Sistemi operativi o Router che quando ricevono un particolare pacchetto (il cui IP di provenienza è uguale a quello di destinazione, cioè l'attaccato) di richiesta di connessione tentano di stabilirla ma vanno incontro ai più diversi blocchi. In pratica l'attaccato cerca di colloquiare con se stesso. L'I-Storm ADSL Router elimina tutti i pacchetti con questa caratteristica.

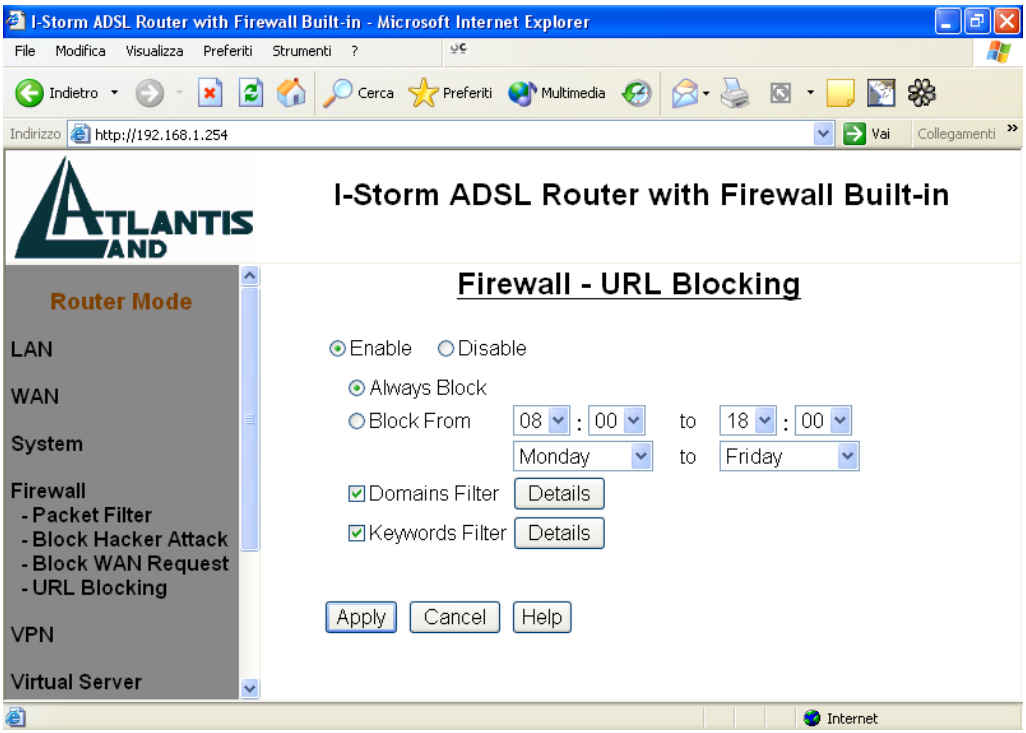
Block WAN Request



Evidenziando "Enable" è possibile evitare di rispondere ai pacchetti di PING che giungono al router dall'esterno. Quelli indirizzati verso l'esterno sono comunque fatti passare.

URL Filter

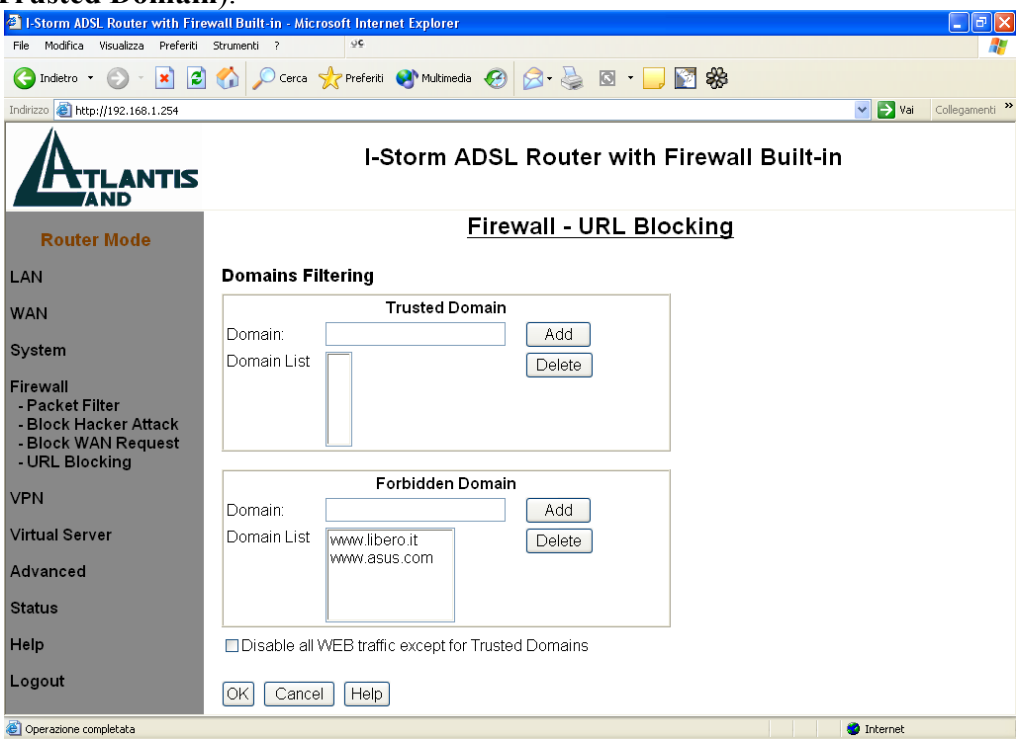
Tramite questa funzionalità è possibile filtrare ulteriormente il traffico in uscita limitando tale traffico in base all'ora e/o giorno ed al tipo di URL. Sarà possibile bloccare l'accesso ad alcuni siti oppure consentire l'accesso solo ad una lista opportuna di siti. E' inoltre possibile impedire l'accesso ad alcuni URL che hanno una determinata sequenza di caratteri.



Scegliendo l'opzione **Always Block** le regole di filtraggio verranno applicate sempre, nel caso invece si scelga **Block From** è possibile limitare, in base al giorno e all'ora l'utilizzo dei filtraggi.

Domains Filter

Un po' come il firewall il concetto del filtraggio applicato ai domini resta identico. E' possibile infatti creare una lista di siti vietati (da mettere in **Forbidden Domain**), oppure consentire l'accesso a solo un limitato numero di siti (da mettere in **Trusted Domain** e spuntare la voce **Disable all Web traffic except for Trusted Domain**).



3.4.5 VPN

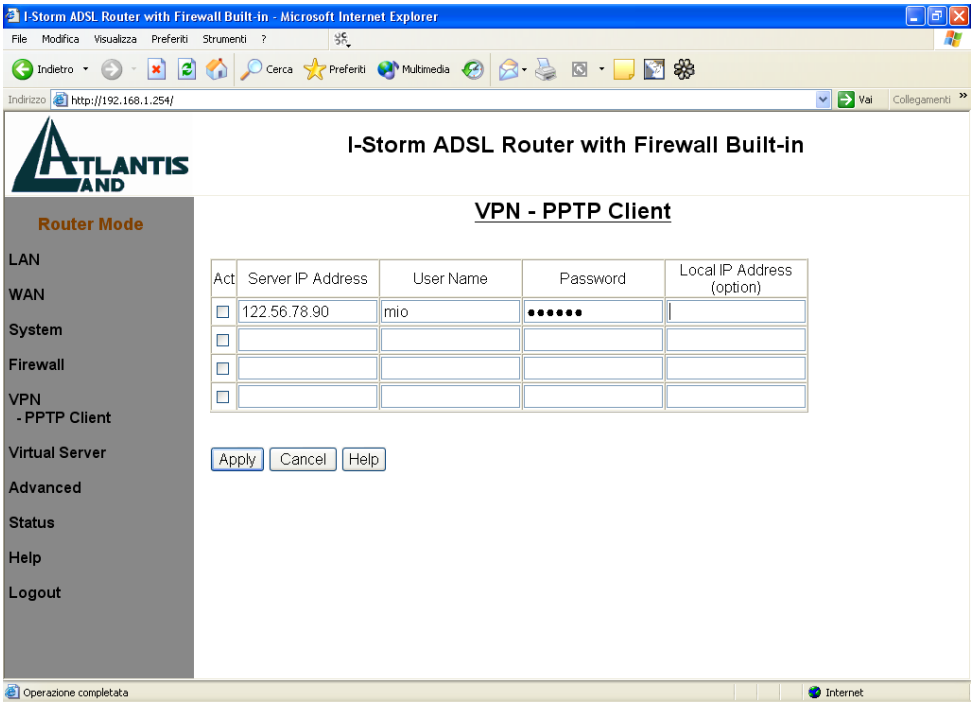
Per prima cosa il termine inglese VPN sta per **Vitual Private Network**, cioè una rete privata virtuale. Il motivo che ha fatto sentire l'esigenza delle VPN risiede nel desiderio di poter collegare in maniera sicura due (o anche un numero maggiore) di Lan private utilizzando come mezzo una rete pubblica (come appunto Internet) per il trasporto dei dati. Le VPN dunque utilizzano le reti pubbliche per trasportare informazioni tra due distinte reti locali. Il grandissimo vantaggio delle VPN risiede nel basso costo (se confrontate con soluzioni come linee dedicate capirete subito che le cifre "risparmiate" diventano davvero importanti). La sicurezza (che rispetto all'uso di una rete privata) diviene però un fattore di assoluta importanza (in fin dei conti usate, per spostare informazioni confidenziali, una rete pubblica). Tutti i dati che viaggiano sulle reti pubbliche devono essere criptati tramite svariati algoritmi atti ad impedirne l'intercettazione, garantirne l'integrità e verificare la loro autenticità. Vediamo meglio queste caratteristiche alla base delle VPN:

Confidenzialità:
Permette che un pacchetto sia ricevuto e leggibile solo e soltanto dal destinario dello stesso (rendendo inefficace l'utilizzo di sniffer da parte di utenti curiosi, che si troverebbero con un pacchetto cifrato e che non saprebbero interpretare). L'intero pacchetto viene pertanto criptato con opportuni algoritmi.

Integrità:
Permette che i dati arrivino a destinazione integri e quindi inalterati durante il tragitto.

Autenticazione:
permette di verificare l'identità del mittente (evitando ad esempio fenomeni di spoofing).

PPTP Client



Una VPN (Virtual Private Network) consente, attraversando Internet ed usando l'IP, l'accesso alle risorse della Lan interna da parte di un utente esterno. Per attivare questa funzionalità è sufficiente attivare l'opzione **Enable.** E' necessario compilare i seguenti campi:

Username: Campo composto da massimo **63** caratteri alfanumerici (case sensitive).

Password: Campo composto da massimo **63** caratteri alfanumerici (case sensitive).

Server IP Address: Introdurre l'indirizzo IP del server PPTP.

E' possibile ottenere l'indirizzo IP dei DNS automaticamente se il server PPTP li fornisce al momento del LogOn. E' altresì possibile che gli indirizzi IP dei DNS non siano forniti in maniera automatica, in questo caso è necessario introdurre tali indirizzi a mano (fare riferimento alla sezione WAN-DNS per maggiori dettagli). Quando si costruisce un tunnel VPN, i DNS attivi non sono quelli della sezione WAN-DNS. A causa del tunnel col server PPTP remoto, la LAN è connessa alla LAN remota direttamente. **Tutti i pacchetti in uscita dalla vostra LAN sono inviati direttamente verso la LAN remota** direttamente e pertanto bisogna settare i DNS coi valori dei DNS del server.

La funzionalità VPN consente di stabilire un tunnel PPTP con un server remoto PPTP e la vostra Lan. Il router deve prima connettersi ad Internet tramite l'ISP prima e poi usare un client PPTP per costruire la VPN.

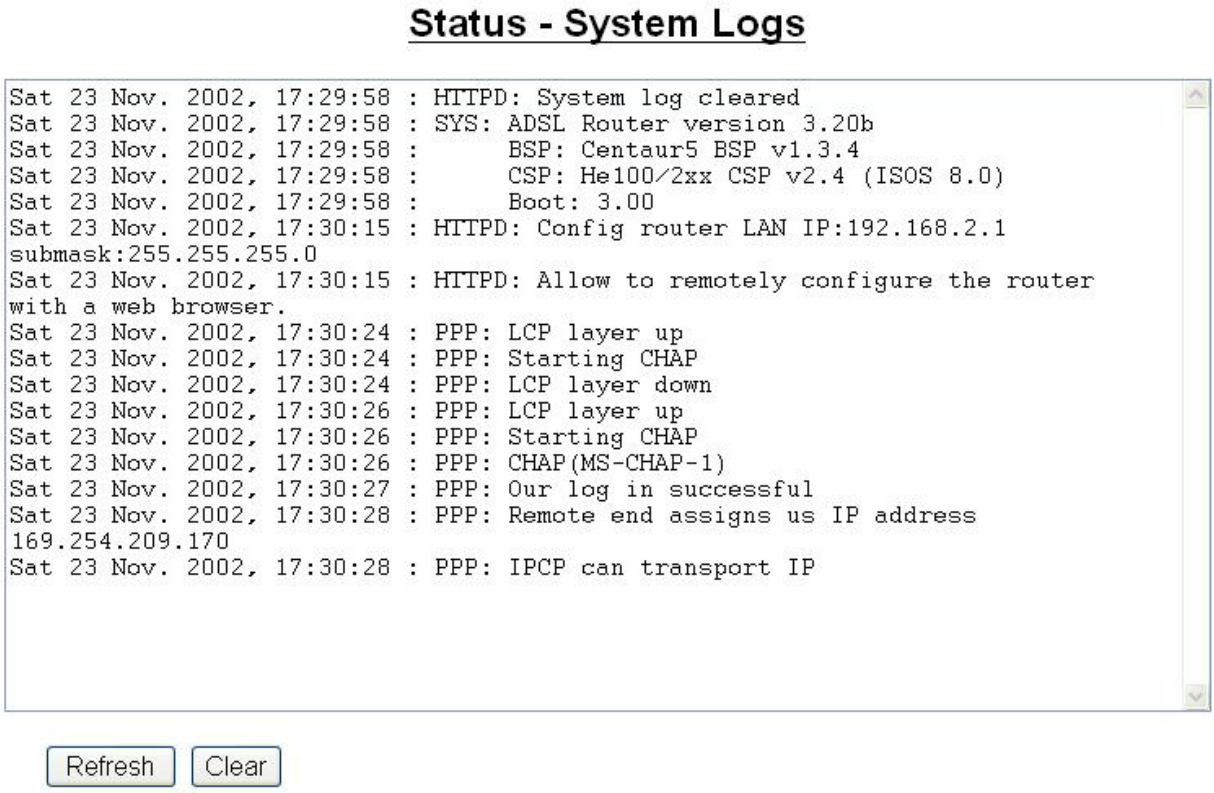
Qualora fosse disabilitato il NAT la funzionalità VPN non sarebbe usabile.

Una volta configurato il PPtP Client (inserito l'IP del PC esterno che fa da server PPtP, l'username e la password) sul Router, spuntate il campo Act e premete Apply. Il Router consentirà ad ogni PC della Lan di usufruire delle risorse della Lan del Server VPN. Andando nella sezione Status-System Status dovreste vedere l'immagine di sotto:

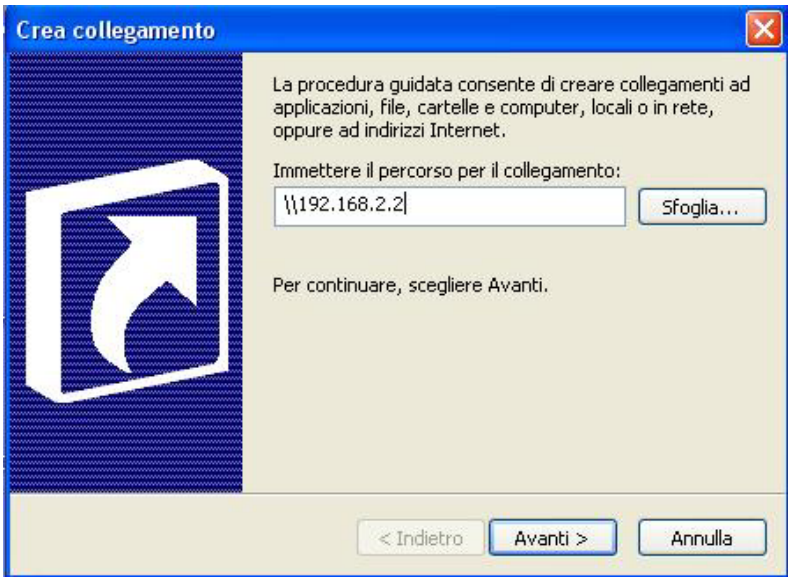
	PPPoA	connected 5 : 2 : 7 [disconnect]
	Last Error Message	
	VPI	8
	VCI	35
	NAT	Enable
	Encapsulation	VC MUX
	IP Address	62.211.137.88
	Gateway Address	192.168.100.1
	PPTP Client 3	Connected [connect]
	Server IP Address	62.10.15.213
	Remote Tunnelling Address	169.254.72.105
	Local Tunnelling Address	169.254.209.170
	DNS Address	212.216.112.112 , 212.216.172.62
ADSL		
	Line Status	showtime
	Last Error Message	
	Downstream Rate	800 kbps (interleaved)
	Upstream Rate	160 kbps (interleaved)
	Tx Packets	0/2 (good/bad)
	Rx Packets	0/0 (good/bad)

[Refresh] [Clear]

In cui è possibile vedere che il **PPTP client 3** è connesso correttamente col server VPN. Ulteriori informazioni sono ottenibili consultando il System Logs (sempre in Status). Dovreste vedere una figura analoga:



A questo punto non resta che creare, su un qualsiasi PC della Lan dietro al Router, un collegamento con l'IP del PC dell'altra Lan per avere accesso alle risorse della macchina. Su Windows XP cliccare il tasto destro,sul Desktop, scegliere **Nuovo** e poi **collegamento**. Vi apparirà la schermata sotto riportata



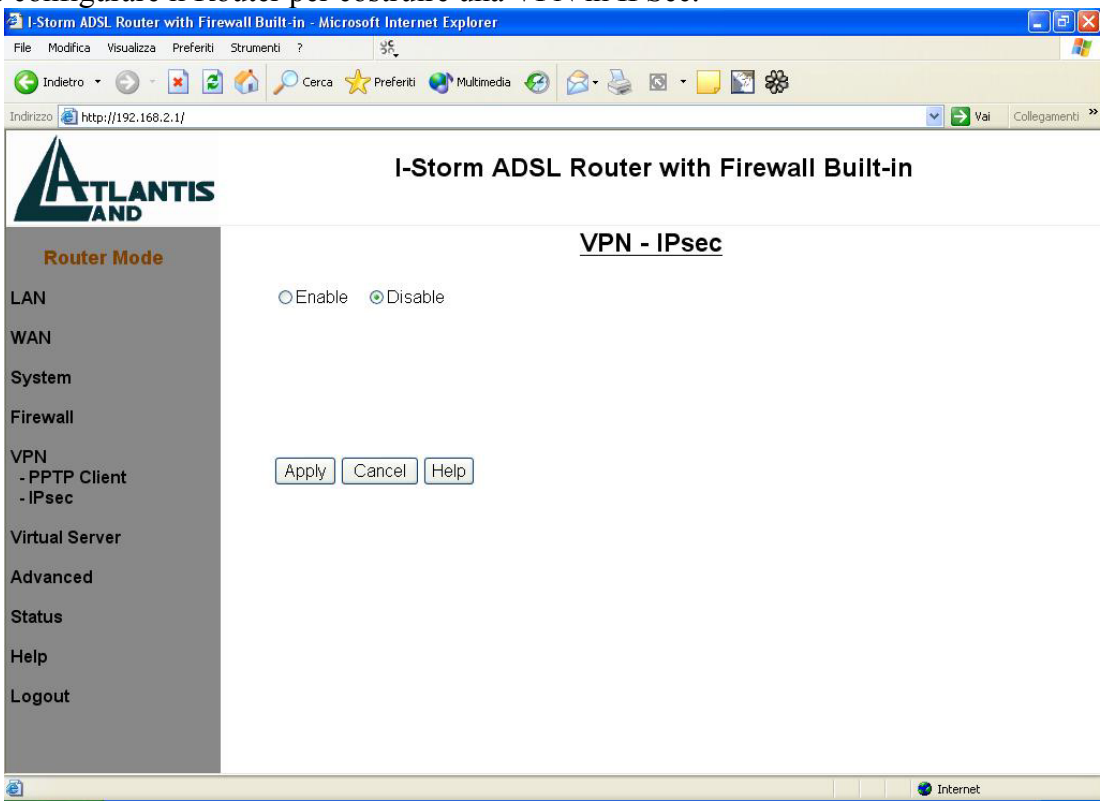
Inserire nel campo vuoto l'indirizzo IP di un PC nella LAN remota per poter accedere alle risorse condivise. Se per esempio si volesse accedere alle risorse del Server bisognerebbe immettere l'IP del Remote tunneling address.

Il Router ADSL è trasparente al passaggio delle VPN in PPTP, se dunque un PC della LAN (con IP privato) stabilisce una VPN con un PC remoto (dotato di IP pubblico), questa sarà costruita. Qualora invece un PC esterno volesse costruire una VPN (chiamando l'IP pubblico WAN del Router) con PC della LAN (con IP privato), questa può essere costruita solo se nella sezione Virtual Server del Router è stata creata una DMZ (vengono ruotati protocolli non gestiti dal VS, che consente la rotazione di solo TCP e UDP) con l'IP privato del PC della LAN con cui si vuole costruire la VPN. Bisogna inoltre prestare particolare attenzione ai protocolli filtrati nella sezione firewall. Infatti Ogni qualvolta entra/esce un pacchetto nel/dal Router questo viene confrontato con le regole del Firewall, una per una, sino a che non ne viene soddisfatta una. Qualora nessuna regola sia stata soddisfatta il pacchetto è inviato. Qualora abbiate seguito un approccio conservativo (generando n regole per far passere ciò che ritenete sicuro e creato una regola n+1 che taglia tutto) può essere che TUTTI i protocolli vengano tagliati dall'ultima regola (se avete scelto ANY). In questo caso, utilizzando altri protocolli, tale regola impedirebbe la costruzione della VPN. Ovviamente è possibile creare una sola VPN (da un PC della Lan o verso un PC della Lan) alla volta date le impossibili rotazioni dei protocolli (non sono basate su porte) utilizzati su più PC.

Durante una VPN in PPTP nella sezione System-Status il conteggio dei pacchetti in entrata/uscita viene interrotto.

VPN IPSec

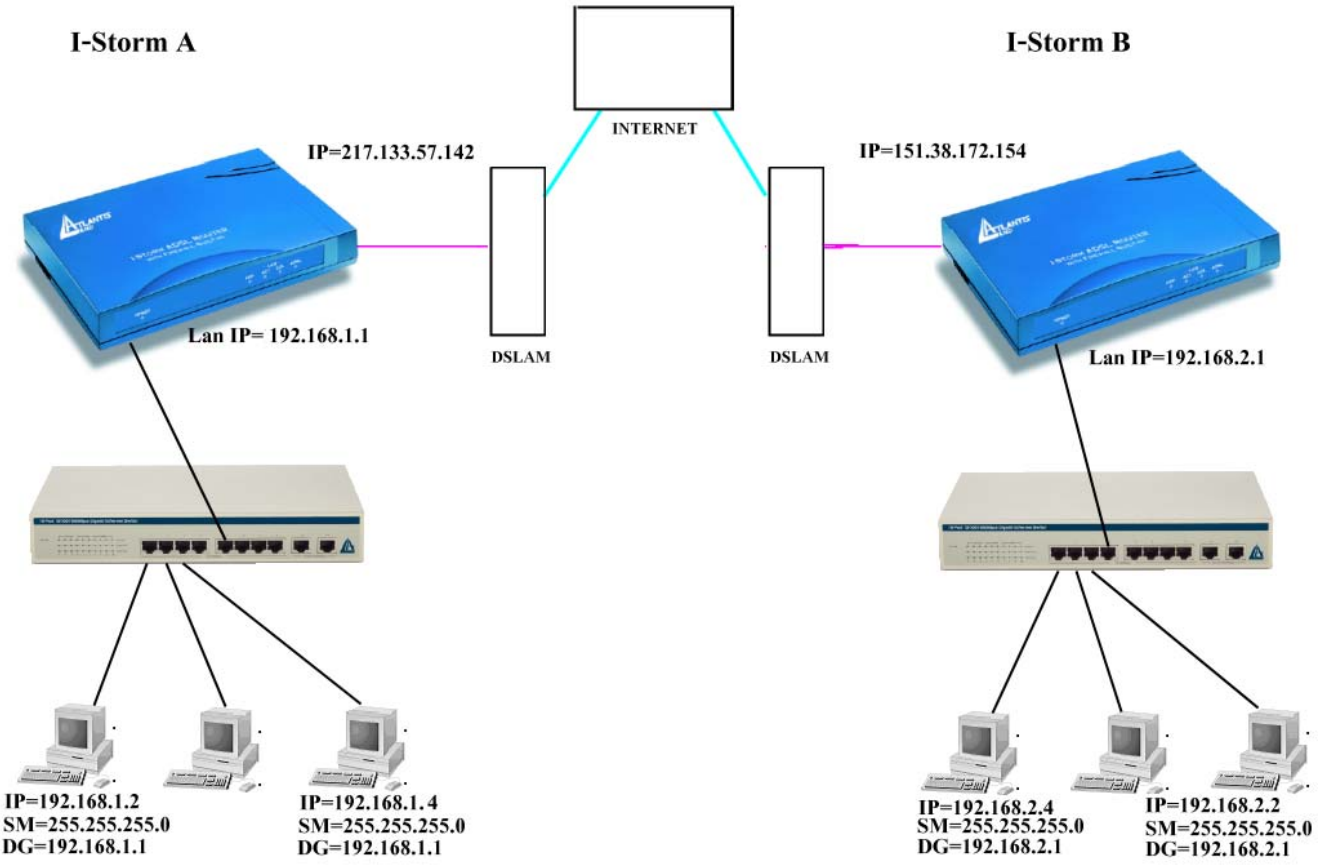
Per creare una VPN in IPSec è sufficiente cliccare sulla voce VPN e poi scegliere IPSec. Vi apparirà la foto sotto riportata in cui sarà sufficiente spuntare la voce enable e premere Apply. A questo punto è possibile configurare il Router per costruire una VPN in IPSec.



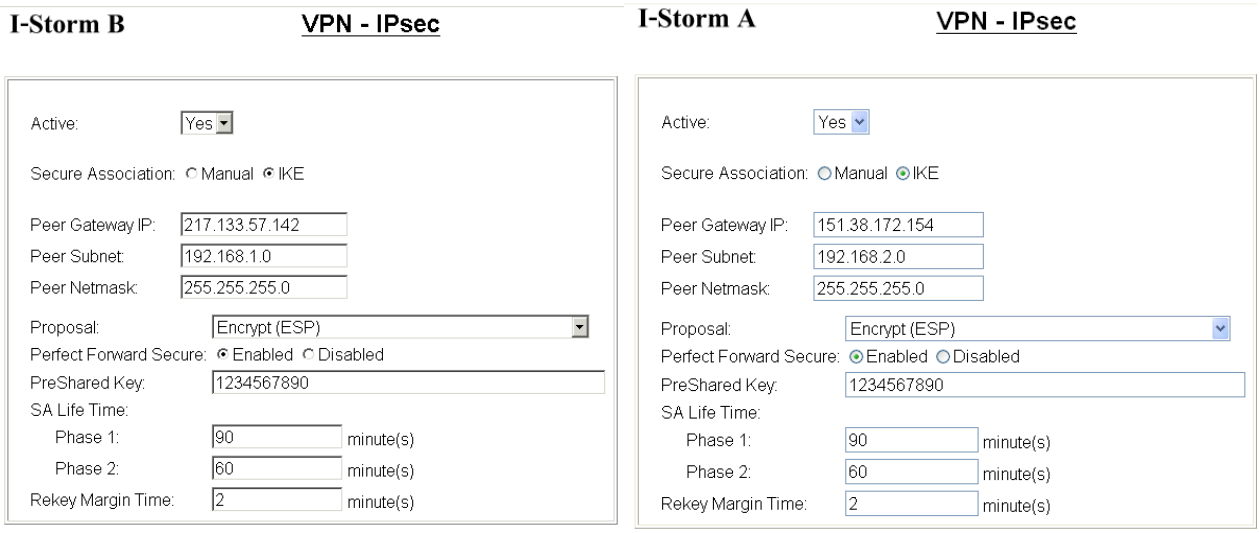
Segue un esempio di configurazione di una VPN in IPSec che consente un collegamento Lan-To-Lan. In questa modalità ogni PC appartenente ad una delle Lan può vedere, in tutta sicurezza, tutti i PC dell'altra Lan.

Per il corretto funzionamento della VPN in IPSec bisogna evitare che le 2 Lan abbiano la stessa subnet.

L'ipotesi di partenza è quella di avere 2 Lan che chiameremo Lan-A e Lan-B entrambe dietro un Router I-Storm ADSL che effettua NAT e dispone di un IP pubblico statico (è possibile la costruzione di una VPN in IPSec con IP dinamico ma va settata di volta in volta, è comunque previsto il rilascio di un firmware che integrerà la gestione DDNS in modo da poter costruire una VPN legata al dominio registrato e non all'IP, che potrà anche essere dinamico).
La figura di sotto dovrebbe chiarire lo schema delle 2 LAN (la LAN-A ha indirizzi privati nella subnet 192.168.1.x e l'IP pubblico del Router A è 217.133.57.142, la LAN-B ha indirizzi privati nella subnet 192.168.2.x e l'IP pubblico del Router B è 151.38.172.154).



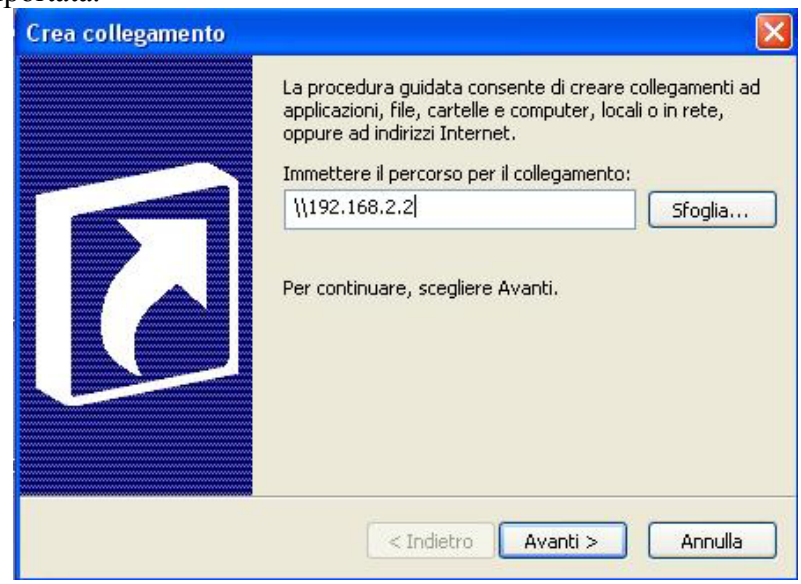
I 2 Router I-Storm vanno configurati come nelle figure riportate sotto.



Dopo qualche minuto, se tutto è stato fatto correttamente avrete realizzato una VPN in IPSec tra le 2 LAN. Per verificare questo provate a pingare da un PC della LAN un PC dell'altra (togliendo dai Router la funzione di **Block Wan Request** nel Firewall).

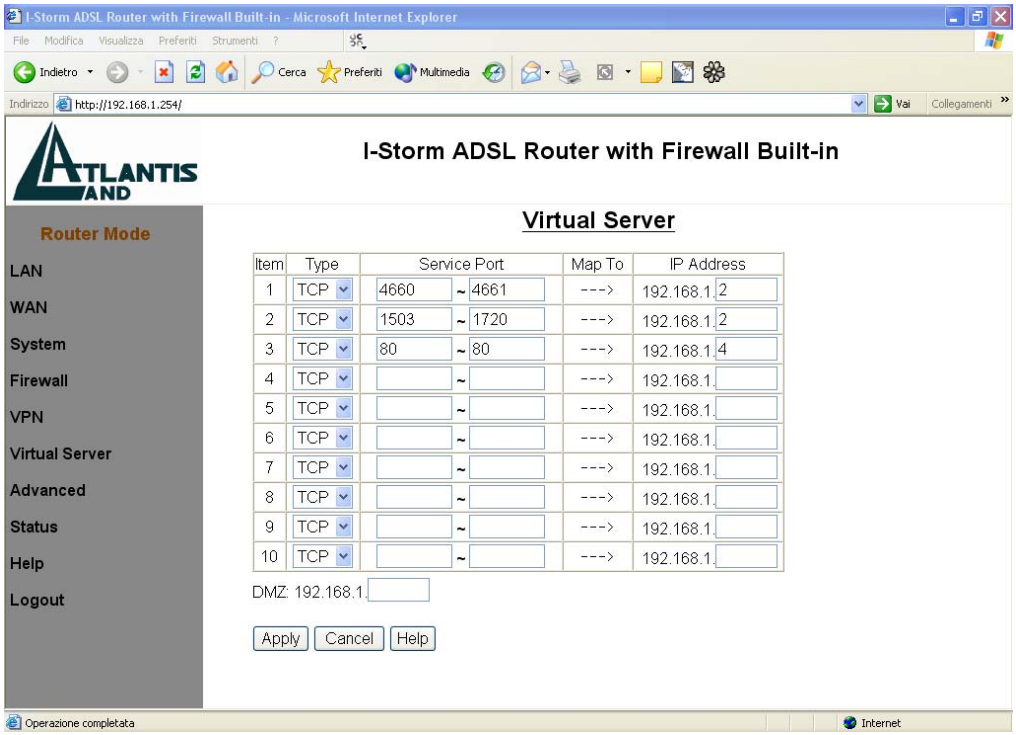
E' possibile condividere, ad esempio, le risorse dei PC creando un collegamento e mettendo l'indirizzo IP (privato) del PC.

Su Windows XP cliccare il tasto destro,sul Desktop, scegliere **Nuovo** e poi **collegamento**. Vi apparirà la schermata sotto riportata.



Inserire nel campo vuoto l'indirizzo IP di un PC nella LAN remota per poter accedere alle risorse condivise. Nell'esempio si è assunto di creare un collegamento da un qualsiasi PC appartenente alla LAN-A verso un PC della LAN- B (il PC con IP=192.168.2.2).

3.4.6 Virtual Server



Il firewall del Router ADSL consente la protezione della LAN locale da parte di accessi indesiderati. Può essere necessario, qualche volta, consentire ad utenti esterni l'accesso ad un PC specifico della Lan (per esempio verso un PC fa da server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta (si ricorda che Web =80, FTP =21, Telnet =23, SMTP =25, POP3 =110, DNS =53, ECHO =7, NNTP =119) , su un PC della Lan interna. E' possibile scegliere l'intervallo (o la singola porta) di porte ed il protocollo (tra TCP,UDP o entrambi) che si intende rigirare sull'indirizzo IP.

Se per esempio il server WEB (che riceverà chiamate sulla porta 80) della LAN ha indirizzo IP privato 192.168.1.2 dovremo editare la regola che consenta questo servizio, che verrà fatta nella seguente maniera:

Type=TCP

Service Port=80 (bisognerà inserire 80,80)

IP Address=192.168.1.2

E' chiaro che in questo caso non dovremo utilizzare il DHCP client sul PC poichè in tal caso non conosceremo l'IP che il server Web potrebbe prendere.
E' importante capire che l'I-Storm ADSL Router esegue, in ordine di numerazione crescente, le associazioni richieste dai vari Virtual Server e solo alla fine (qualora fosse presente) rigira il tutto al DMZ. Pertanto se la porta (20)21 è mappata su un certo PC della rete tramite Virtual Server, il PC il cui indirizzo è indicato nel DMZ non potrà funzionare come server FTP.
DMZ: E' a tutti gli effetti un computer esposto ad Internet, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server).

Qualora l'opzione di NAT sia disabilitata nella sezione WAN-ISP, la funzionalità di Virtual Server non è utilizzabile.

Se sul Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual Server per evitare conflitti. In questo caso è sufficiente assegnare al Virtual Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Router ADSL) ed i server DNS) un indirizzo IP che sia nella stessa subnet del Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router ADSL.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del Router ADSL. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consulare eventuali aggiornamenti di questo manuale (scaricabile dal sito www.atlantisland.it o www.atlantis-land.com poi sezioni prodotti, si sceglie il Router ADSL e da qui è possibile scaricare il manuale)

Applicazione	**Settaggi connessioni Uscenti**	**Settaggi connessioni Entranti**
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey	Nessuno	principalmente 4660-4662 TCP , 4665 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190

Usando NetMeeting (Versione3.0), ad esempio, quando la chiamata generata è uscente da un PC dietro al Router verso un PC esterno non ci sono problemi. Il contrario non è realizzabile. Rigirando invece le porte 1503 e 1720 è possibile ricevere anche chiamate in ingresso con video

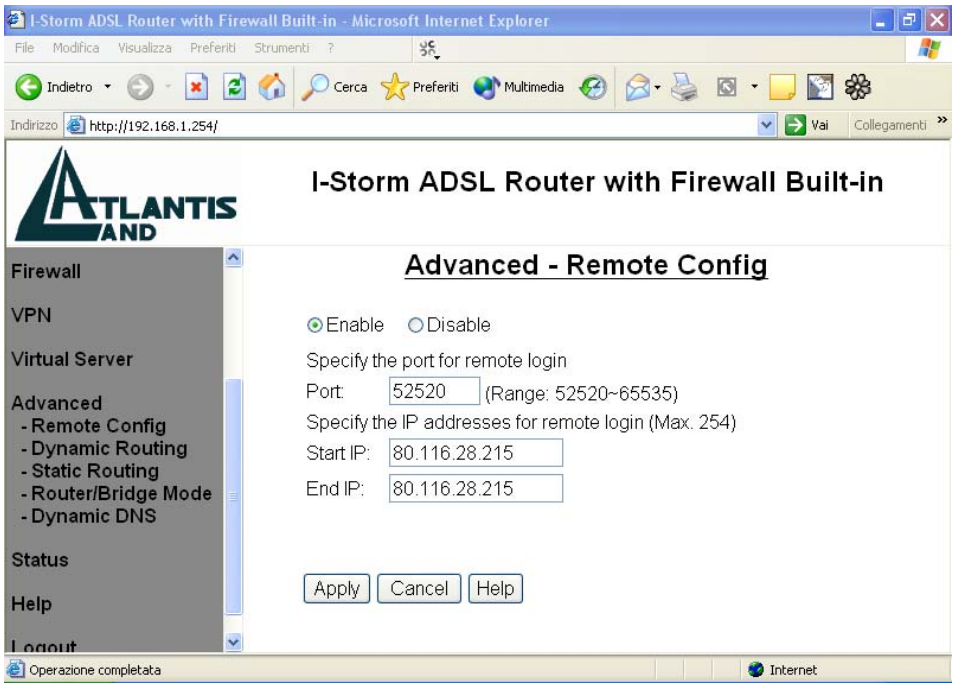
Attenzione il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range potrebbero sorgere problemi ed il servizio di VS funzionare in maniera impropria.

Sono allegate tutta una serie di porte notevoli (da utilizzarsi per il VS ed il Firewall):

Servizio	**Numero di Porta / Protocollo**
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

3.4.7 Advanced

Remote Config



Cliccare su **Enable** qualora si desiderasse la configurazione via browser da Internet.

Per accedere alla configurazione remota digitare nell'URL del browser la seguente stringa:*http://Indirizzo WAN IP :52523, dove WAN IP* è l'indirizzo IP pubblico del Router ADSL. E' consigliabile cambiare il valore della porta al pari della password di entrata per incrementare il livello di sicurezza. Il valore di default è **: 52520**. Bisogna inoltre obbligatoriamente inserire l'IP (dalla release V3.0 del firmware) da cui si desidera effettuare la configurazione remota (al fine di incrementare la sicurezza).

E' possibile fare la prova immediatamente anche dalla propria Lan seguendo i seguenti steps:

1-Andare nella sezione **STATUS** e poi la sottosezione **SYSTEM STATUS**

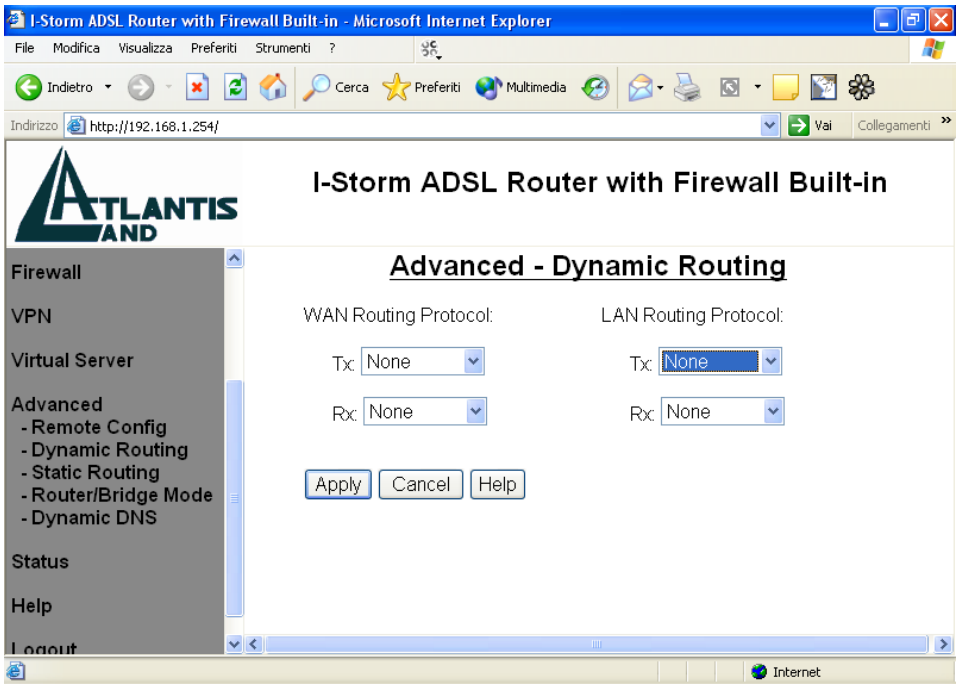
2-Leggere l'indirizzo **IP Address** sotto la sezione **WAN**, ed annotarlo (configurare Advanced Remote settings mettendo tale IP tra quelli che possono controllare da remoto il Router)

3-Chiudere il browser con cui si sta accedendo alla configurazione del Router

4-Riaprirlo e digitare nell'Url**:** *http://Indirizzo WAN IP :numero porta scelta*

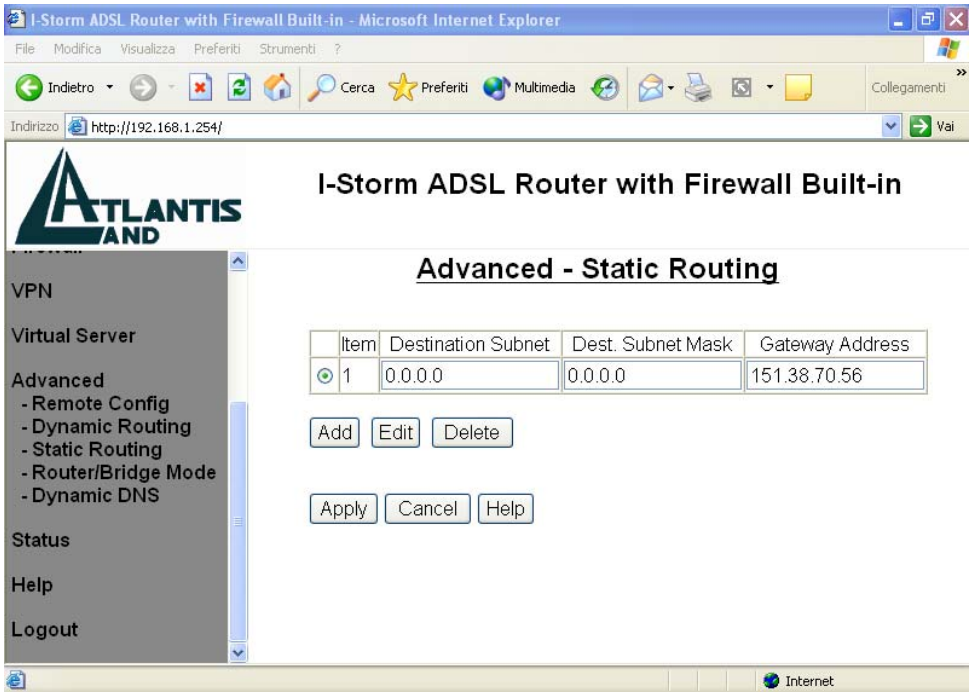
Qualora la funzionalità NAT fosse disabilitata, come indirizzo IP quando si accede alla configurazione del Router bisognerà indicare l'indirizzo della porta LAN del Router ADSL. Tale valore lo si può trovare in System Status.

Dynamic Routing



La funzionalità di Routing dinamico può essere usata per consentire al Router ADSL di regolarsi automaticamente come conseguenza di cambiamenti nello schema della rete. Il Router ADSL usa il protocollo dinamico RIP per svolgere questa funzionalità, infatti fa il broadcasting di queste informazioni agli altri router che aggiustano le loro tabelle. E' necessario scegliere tra RIP1, RIP2 oppure RIP1+RIP2 sia per la trasmissione che per la ricezione attraverso la rete.

Static Routing

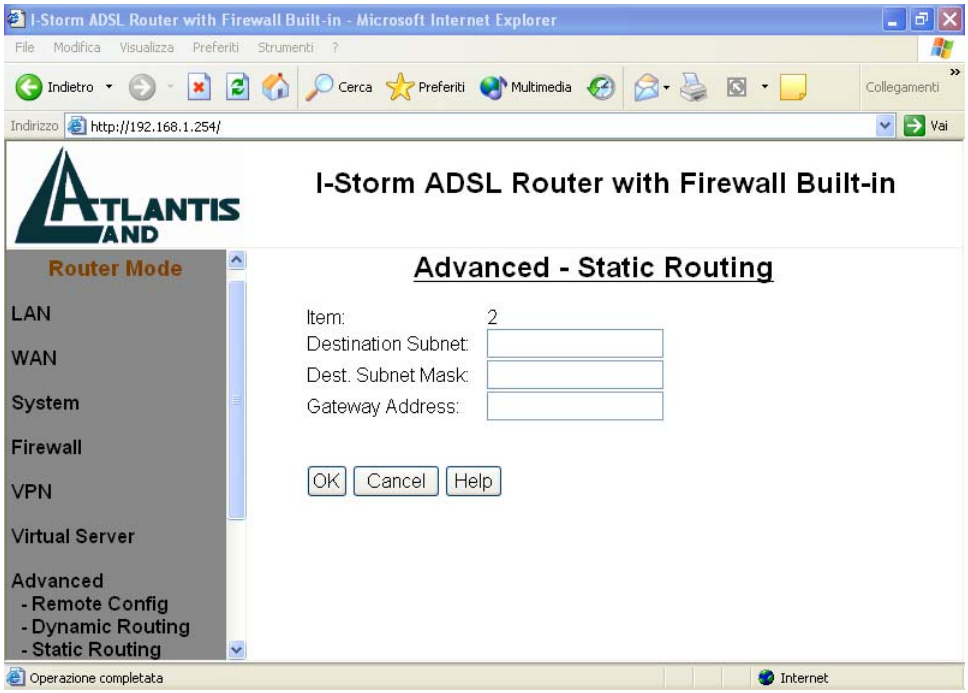


Qualora si avesse un altro Router con una connessione di tipo LAN-to_LAN è necessario creare una istanza nella tabella di routing statico nel Router connesso con Internet.

Add: Cliccare questo bottone per aggiungere una nuova istanza di routine statica. Apparirà la maschera sottostante:

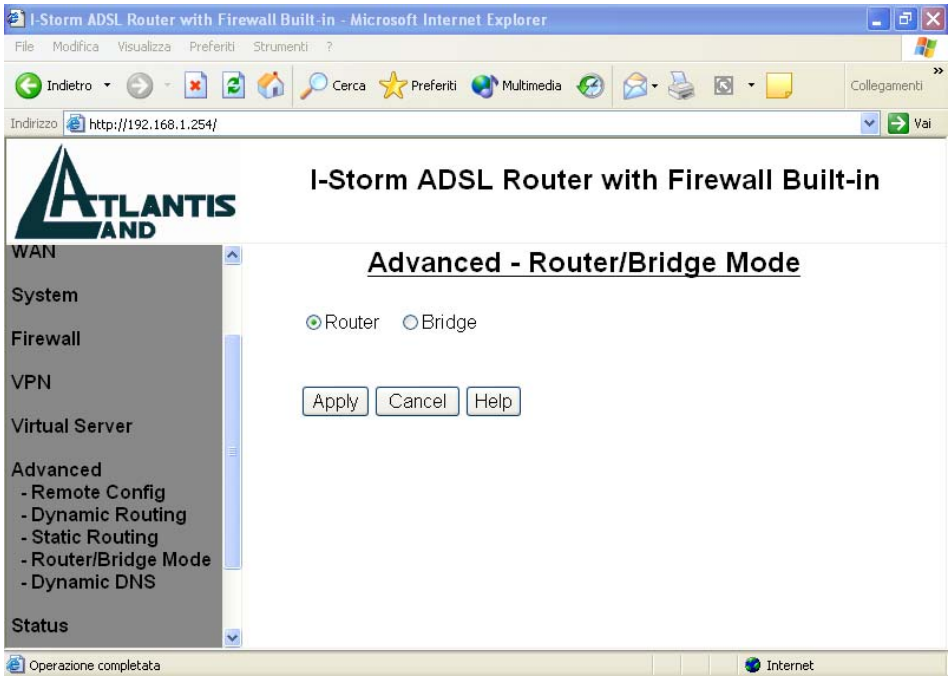
Edit: Selezionare l'istanza da cambiare e poi cliccare sul bottone EDIT.

Delete: Selezionare l'istanza da cancellare e poi cliccare sul bottone DELETE.



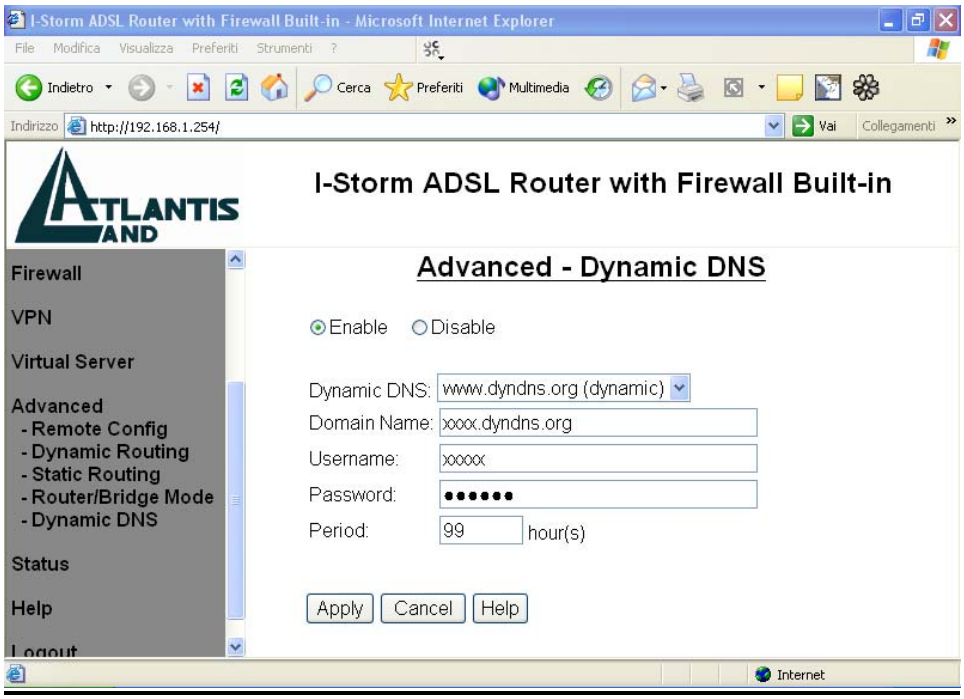
Destination Subnet / Subnet Mask / Gateway Address: Riempire questi campi necessari per questa funzione.

Router/Bridge Mode



E' possibili fare lo switch tra queste due modalità.

Dynamic DNS



Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnetterà, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile ospitare un sito WEB sul proprio PC. I passaggi da seguire sono i seguenti:

1-Registrare il proprio dominio gratuitamente e istantaneamente su www.dyndns.org, www.zoneedit.com.

2-Configurare il client sull'I-Storm Router ADSL inserendo i campi appropriati (Domain Name, Username e Password)

3-Predisporre il PC che deve fungere da server

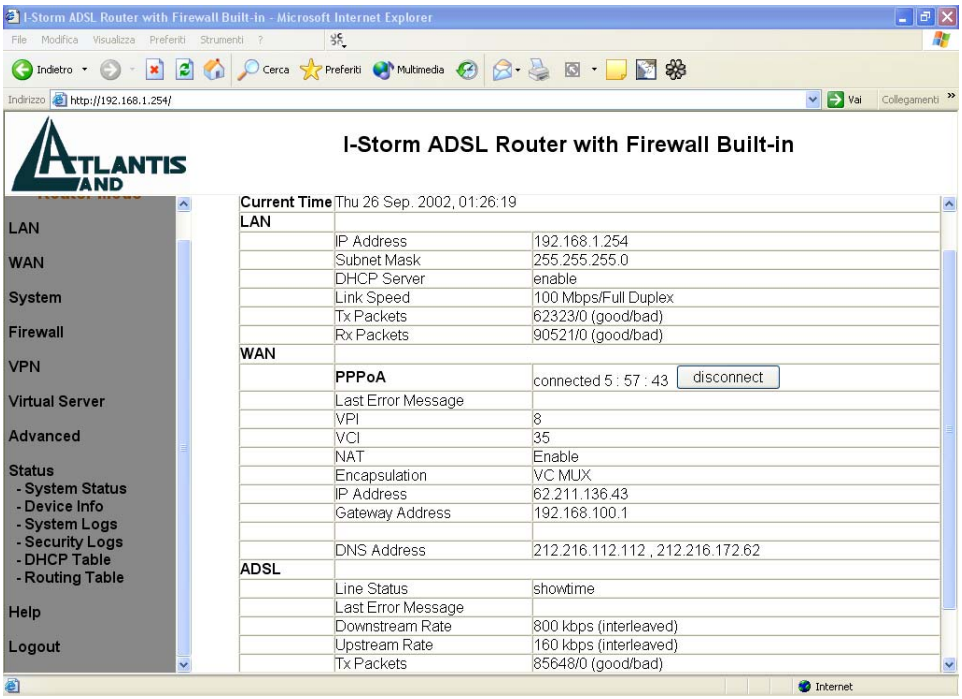
4-Configurare il Virtual Server affinché rigiri sull'indirizzo IP del PC (di sopra) predisposto le connessioni provenienti dall'esterno

In questo modo ogni utente che voglia connettersi al vostro dominio interrogherà il server DNS che gli restituirà di volta in volta l'indirizzo IP assegnatovi dall'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente. In questo modo se il PC resta sempre acceso il server WEB è di fatto sempre raggiungibile(se si escludono problemi diversi).

*Qualora dovreste incontrare problemi quali la sospensione del servizio configurare la voce **Period** a 99 ore, come da figura.*

3.4.8 Status

System Status



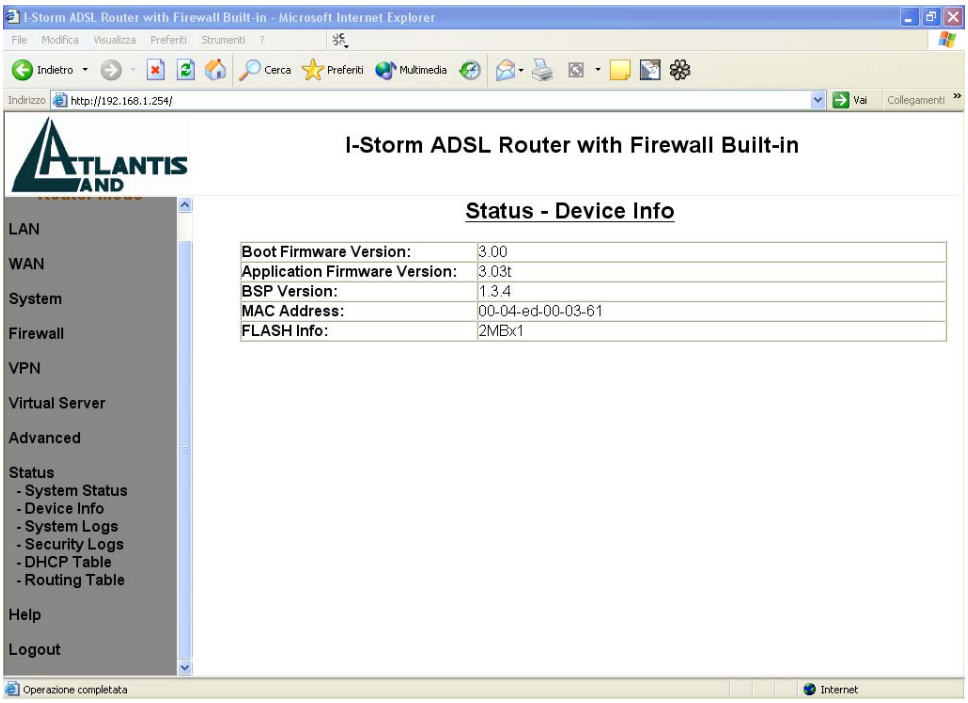
Mostra tutta una serie di informazioni sulla LAN, WAN e lo stato della connessione ADSL.

Nella prima linea, della sezione WAN, si può osservare il protocollo che si sta usando per la connessione ADSL e, ancora più a destra, lo stato di questa. Lo stato del bottone deve essere DISCONNECT, in caso contrario premerlo per poter attivare la connessione.

Coi protocolli PPPoE e PPPoA prestare particolare attenzione al bottone (allo stato della connessione ed al bottone di connessione ancora più a destra). Quando lo stato (vicino al bottone) PPPoE/PPPoA è disconnesso il bottone CONNET consentirà la connessione, altrimenti non realizzabile. Quando il bottone è DISCONNECT lo stato può variare ma la connessione è realizzabile. Lo stato del bottone rappresenta lo stato cui si arriva premendolo, non lo stato attuale (se, per esempio, si è connessi il bottone sarà nello stato DISCONNECT).

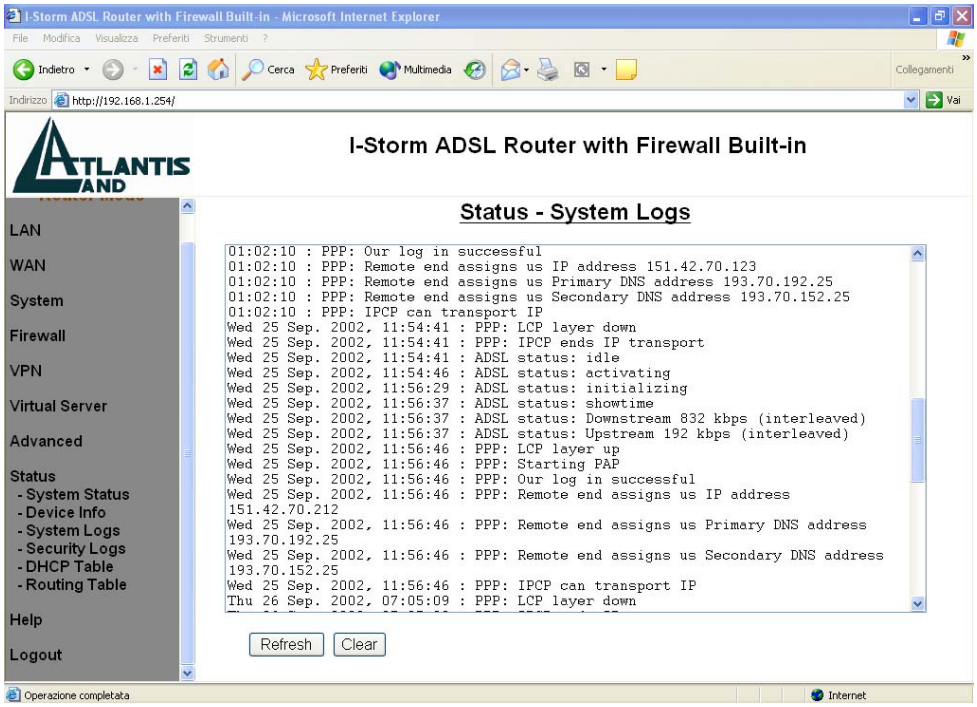
Questa pagina viene aggiornata ogni 15 secondi, cliccando sul bottone di REFRESH si otterrà invece un aggiornamento istantaneo.

Device Info



Mostra le versione di FirmWare e l'indirizzo MAC del Router ADSL.

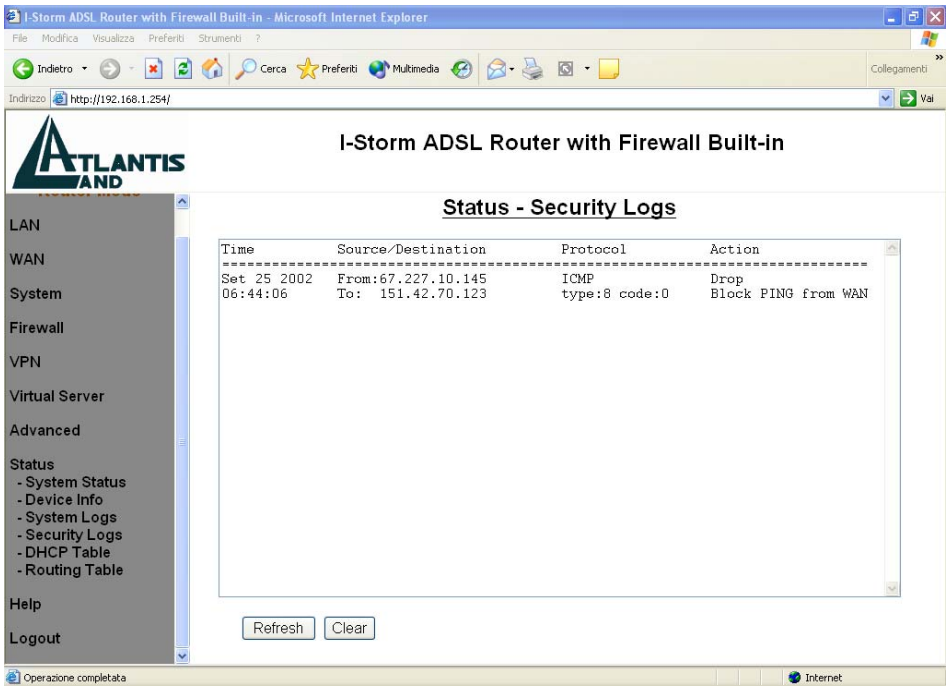
System Logs



Mostra tutte le informazioni storiche relative ai system logs.

Refresh / Clear: Cliccare su **Refresh** per vedere le ultime informazioni del system logs oppure cliccare su **Clear** per cancellare tutte le informazioni relative al system logs mostrate sullo schermo.

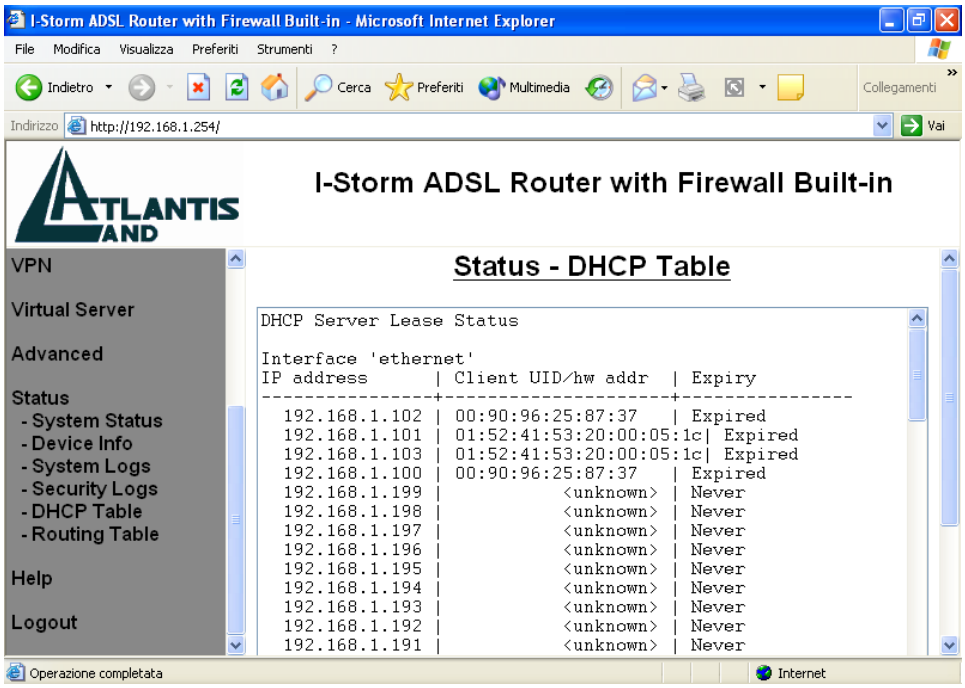
Security Logs



Mostra le informazioni relative a tutto quello che riguarda la sicurezza. Vengono registrate qui infatti tutte le attività del firewall. Ogni regola soddisfatta viene registrata qui assieme agli attacchi di hacker. In questo modo potrete conoscere chi vi ha attaccato (l'IP) e quando e come operano le regole di filtraggio. Quando nuove regole vengono applicate alla sezione firewall la sezione viene svuotata.

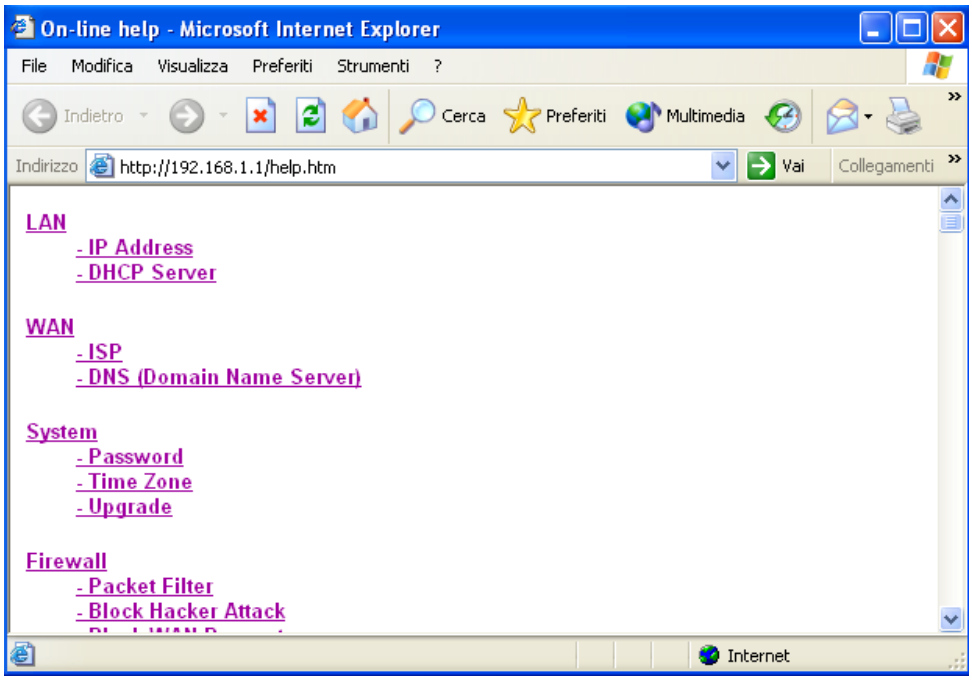
Refresh: Cliccare su **Refresh** per ottenere le ultime informazioni.

DHCP Table



Mostra gli indirizzi IP allocati tramite il server DHCP del Router, se attivo. Consultare, per approfondimenti, la sezione ***3.4.1 DHCP Server.***

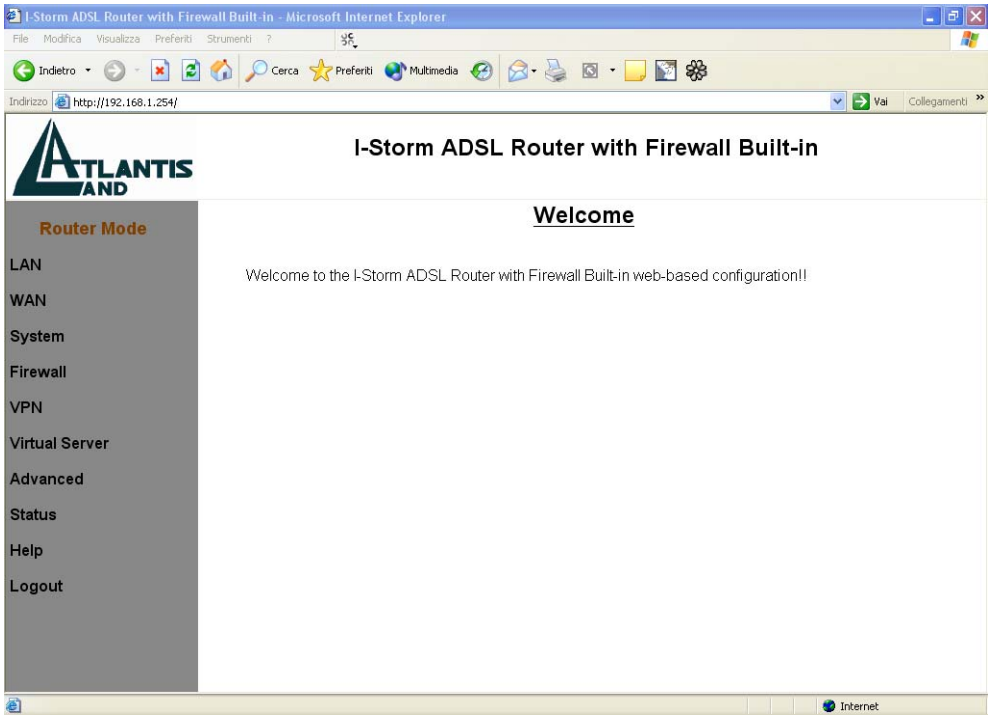
3.4.9 Help



Premendo il bottone HELP, indipendentemente dalla sezione, vi apparirà un breve aiuto che vuole essere non un sostitutivo di questo manuale ma solo un promemoria delle varie voci che troverete nella configurazione del Router ADSL.

3.4.10 Logout

Per uscire dalla configurazione del Router ADSL si consiglia di non chiudere il browser semplicemente ma di effettuare il Logout, ciccando sull'apposita voce (l'ultima verso il basso).



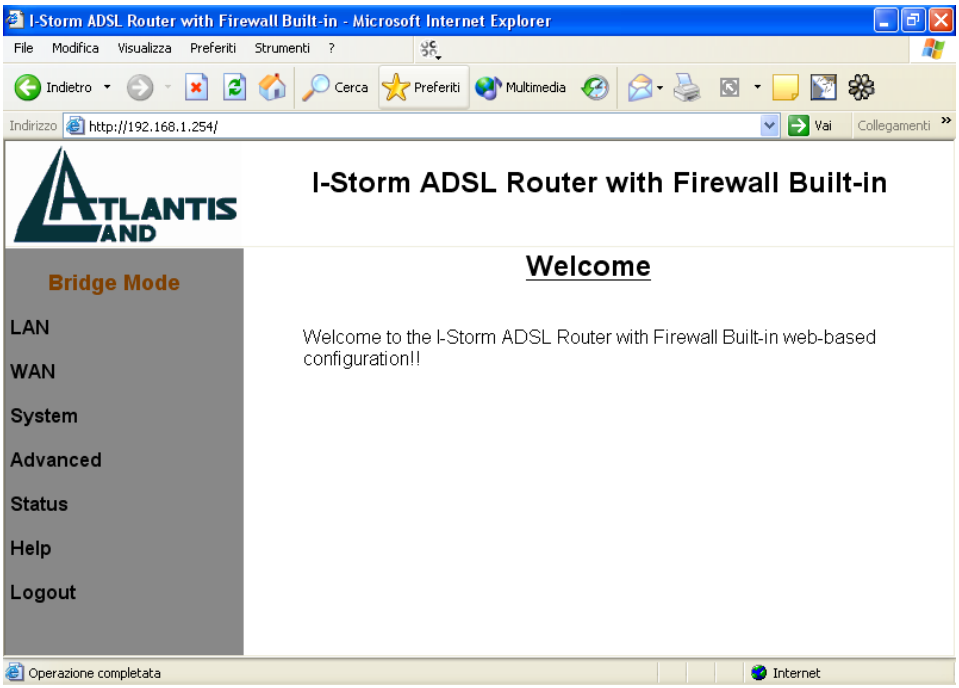
3.5 Configurazione in modalità Bridge Mode tramite browser.

Quando viene fatto funzionare in modalità bridge molte funzionalità (su tutte il firewall) vengono disabilitate. Tale funzionalità potrebbe rendersi necessaria per il funzionamento di alcune particolari applicazioni internet.

Accedere col browser web al seguente indirizzo IP (dove si inserisce l'URL) che di default è: **192.168.1.254**, e premere il tasto invio.

Nessun User Name o Password è richiesta (nel caso di primo accesso). Qualora la password fosse stata cambiata bisogna invece inserirla. Premere **OK** per continuare.

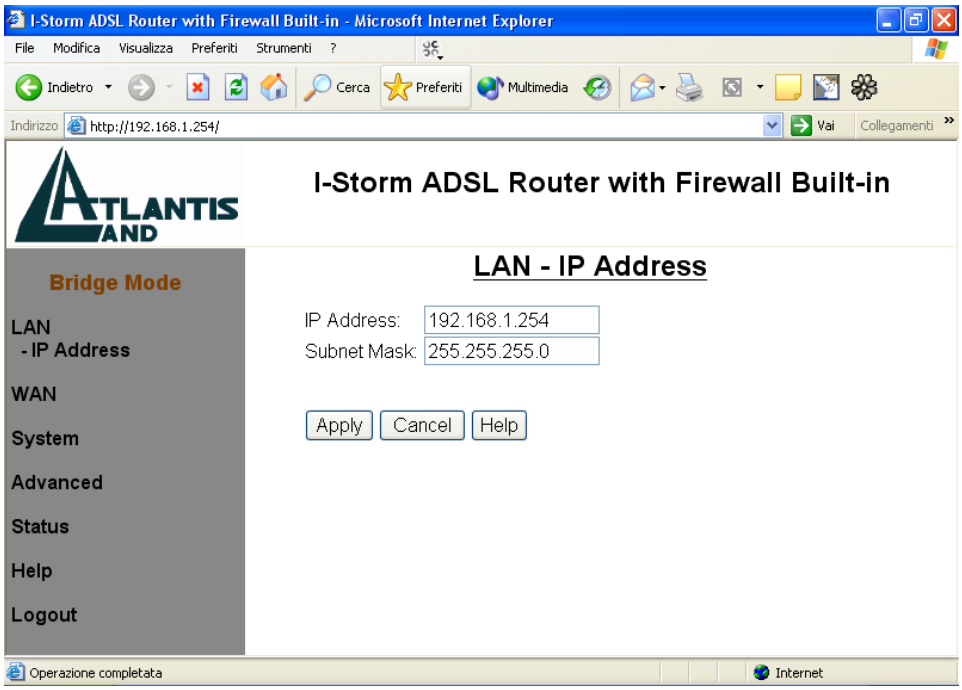
Apparirà a questo punto il Menù Principale, nella parte sinistra si potrà accedere (come se si stessero vedendo i links in una homepage) a tutte le sezioni: **LAN, WAN, System, Advanced, Status, Help** ed infine **Logout**.



Cliccando sulla sezione desiderata, si vedrà nello spazio centrale della homepage tutti i settaggi relativi alla configurazione della sezione scelta.

3.5.1 LAN

Questa sezione contiene i settaggi per la LAN interna. Selezionandola apparirà la sottosezione **IP Address.**



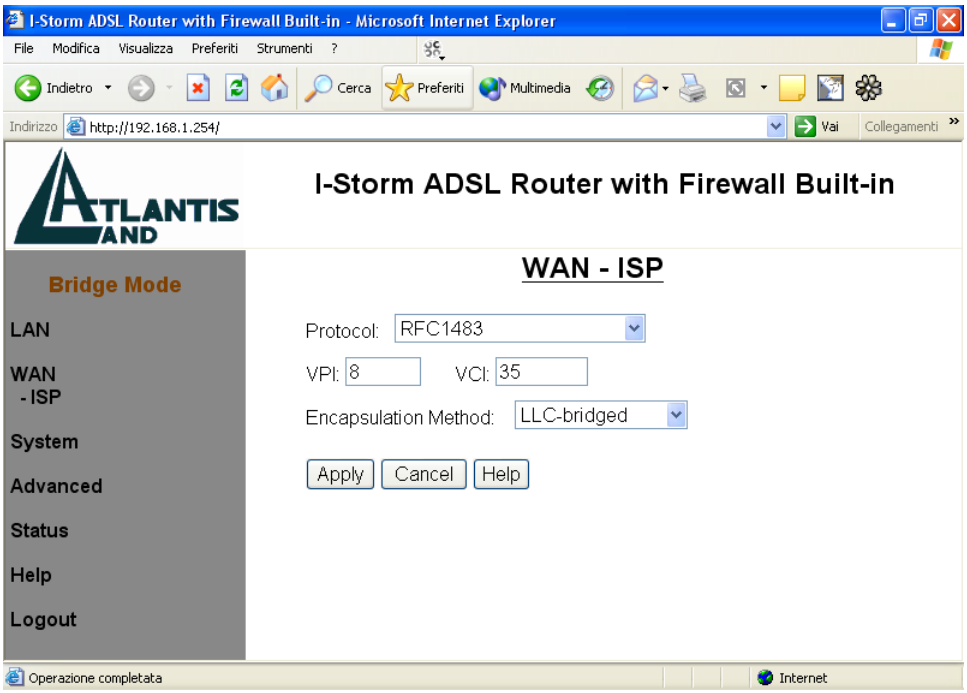
IP Address: Il valore di default è:**192.168.1.254**

Questo è l'indirizzo IP con cui il Router ADSL è visto nella LAN. E' necessario, qualora si cambiasse IP con quello di un'altra subnet accertarsi che tutti I PC della LAN abbiano un indirizzo IP (se non sono settati come client DHCP). Diversamente questo potrebbe impedire il corretto funzionamento della LAN e l'accesso al Router ADSL.

Subnet Mask: Il valore di default è:**255.255.255.0**

3.5.2 WAN

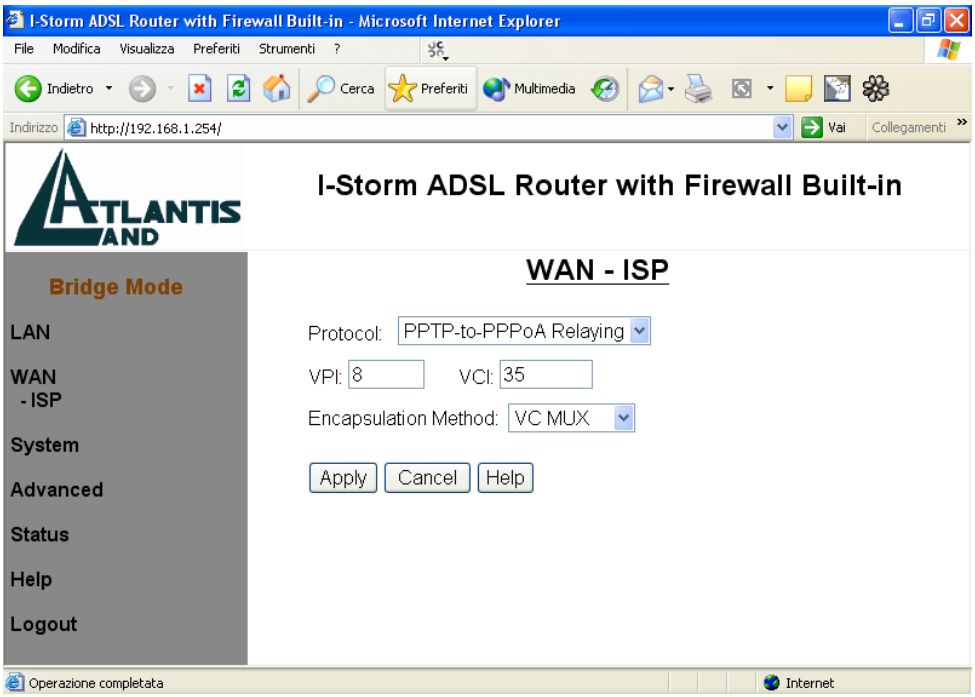
Questa sezione contiene i settaggi per la WAN. Selezionandola apparirà la sottosezione: **ISP.** Dovremo quindi configurare il tipo di connessione ADSL.



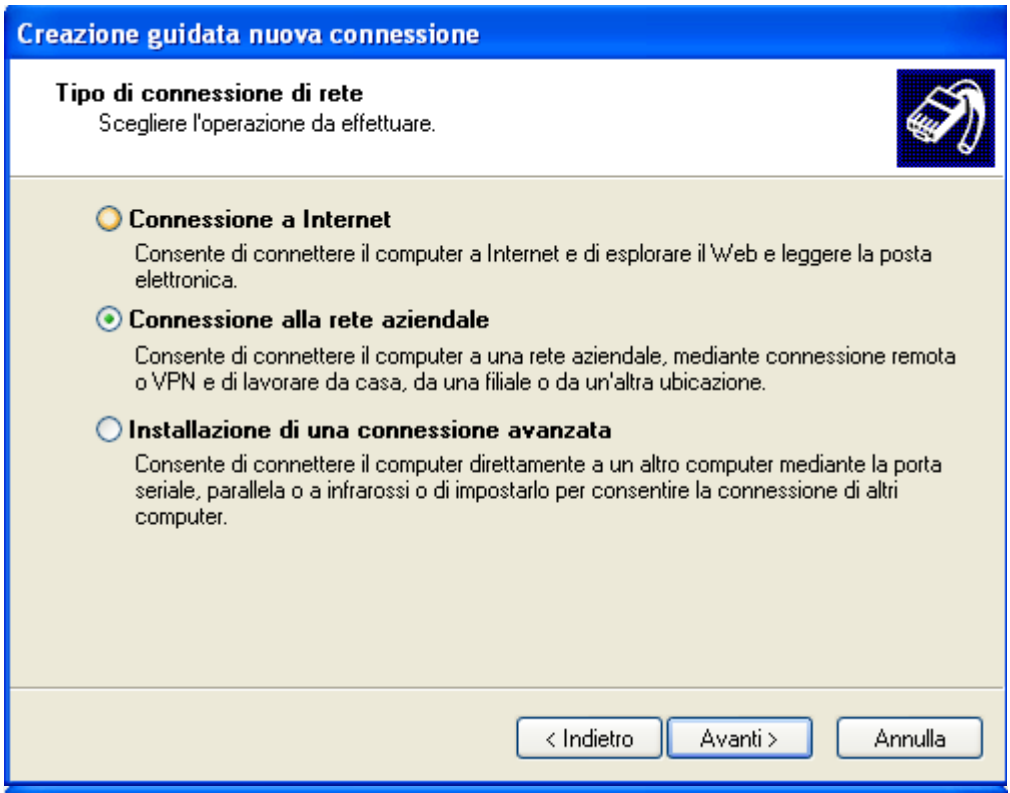
Protocol: Sono soltanto due protocolli rispettivamente **RFC1483** e **PPTP-to-PPPoA Relaying**. E' necessario conoscere quale protocollo è adottato dal vostro provider.
VPI/VCI: Consultare il vostro ISP per conoscere i valori del Virtual Path Identifier (VPI) e del Virtual Channel Identifier (VCI). Il range valido per il VPI va da 0 a 255 e per il VCI da 32 a 65535. I valori di default per il VPI è 8 e per il VCI è 35.

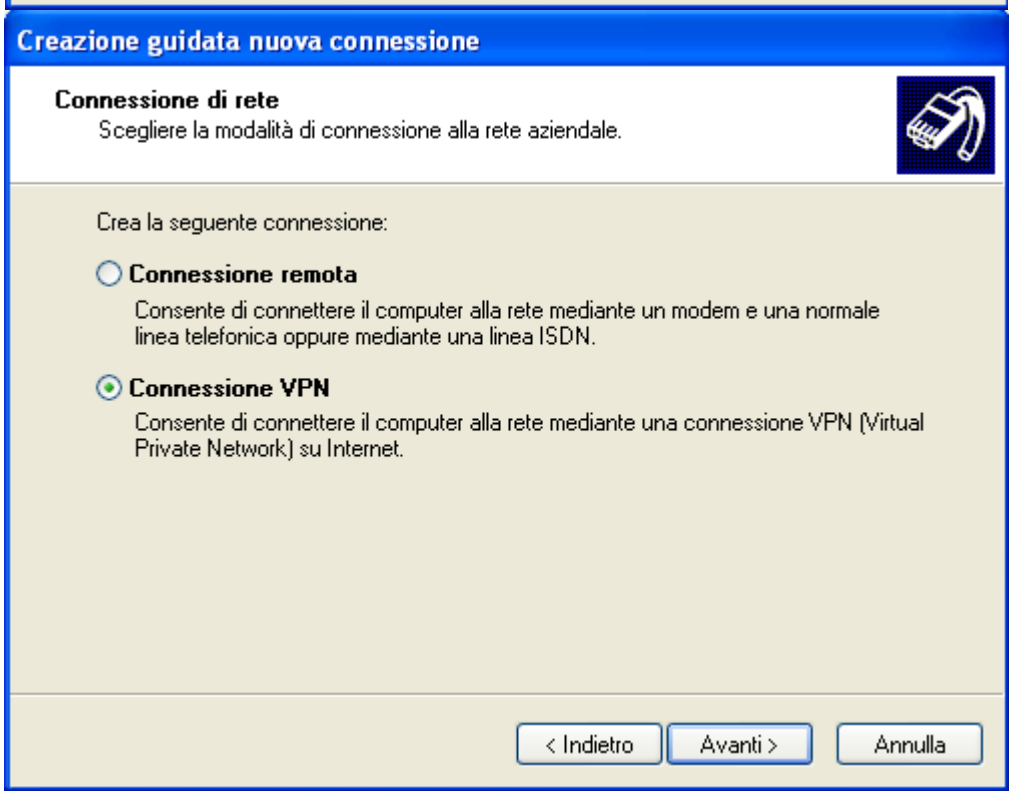
Encapsulation Method: Assicurarsi di usare lo stesso metodo di incapsulamento usato dall'ISP (LLC/SNAP or VC MUX).

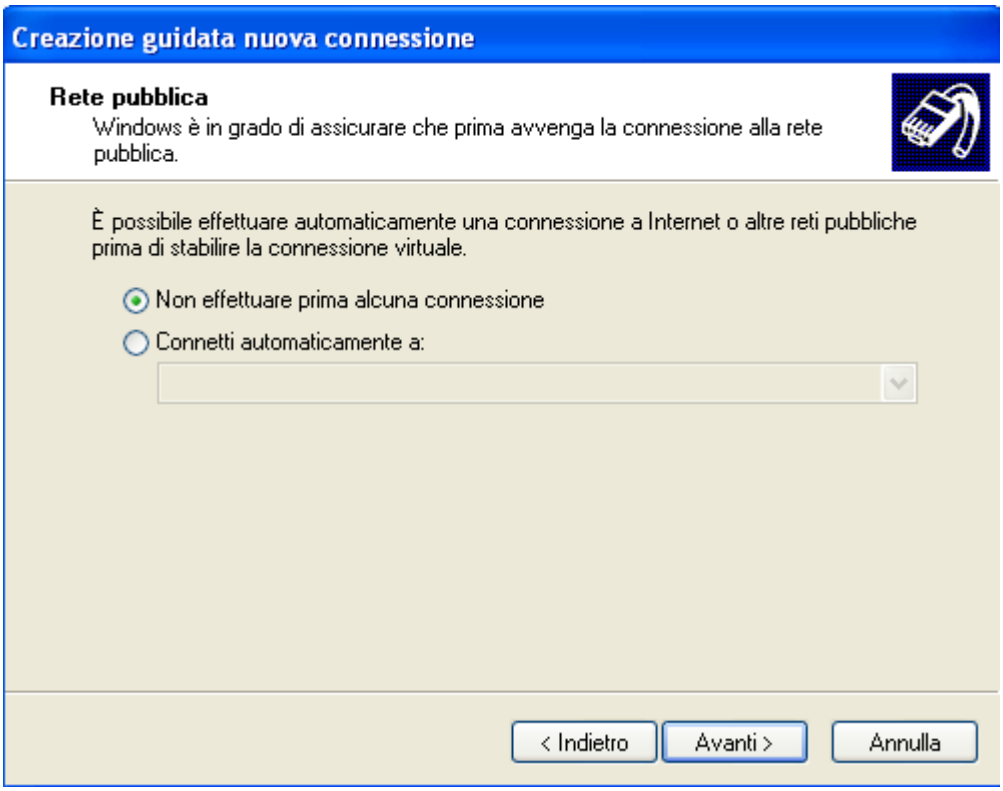
Qualora si utilizzasse il protocollo **PPTP-to-PPPoA Relaying** è necessario creare un acceso di tipo VPN dal PC indicando l'indirizzo IP quello LAN IP del Router ed inserendo username e password dati dall'ISP (come se si stesse facendo una connessione remota).



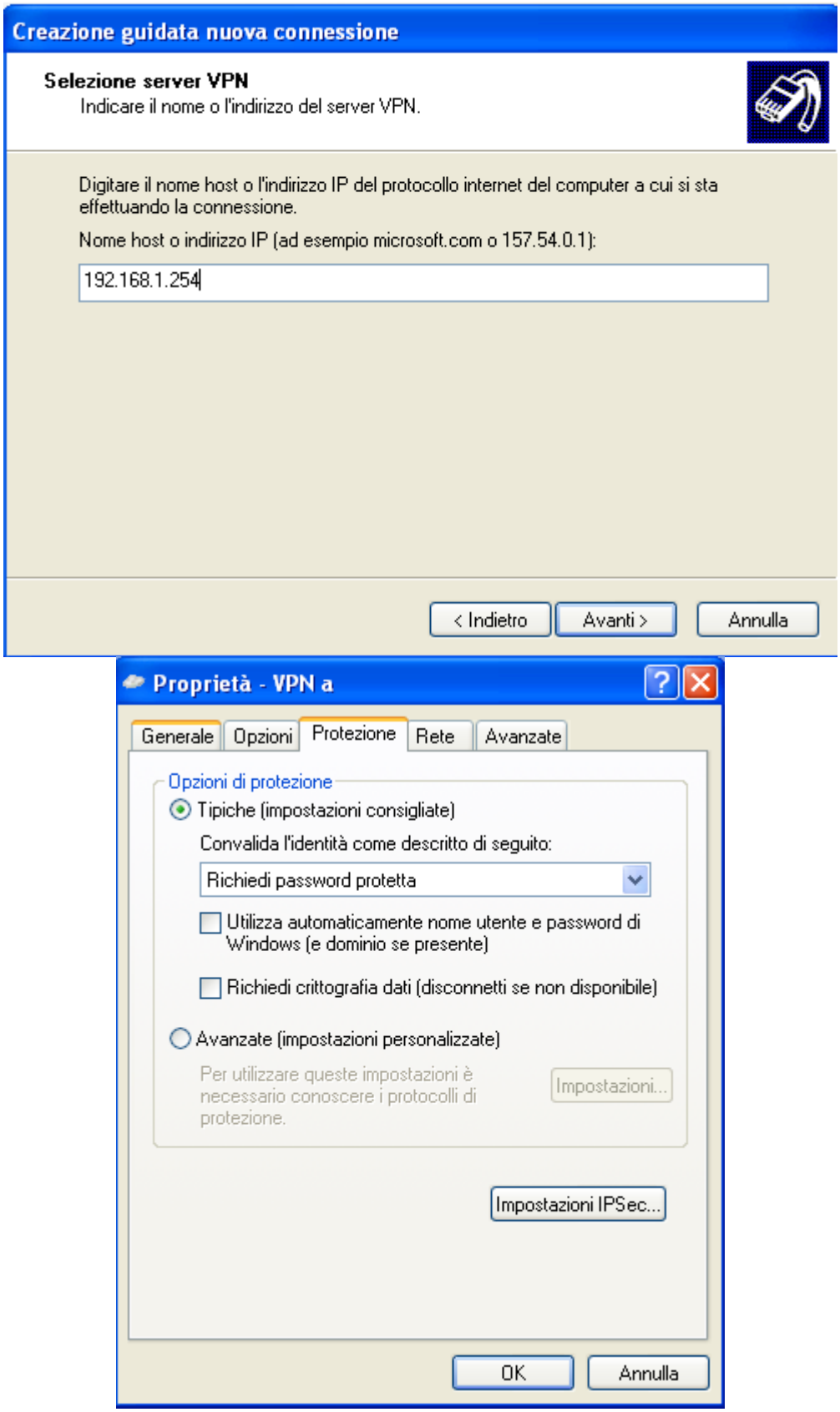
Vediamo nel dettaglio l'esempio della costruzione di una VPN con Windows XP. Anzitutto cliccare sull'icona Connessione di rete contenuta nel pannello di controllo. Poi scegliere la voce crea nuova connessione, premere poi avanti ed effettuare poi le scelte nelle figure seguenti.


Creazione guidata nuova connessione
Tipo di connessione di rete
Scegliere l'operazione da effettuare.
Connessione a Internet
Consente di connettere il computer a Internet e di esplorare il Web e leggere la posta elettronica.
Connessione alla rete aziendale
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.
Installazione di una connessione avanzata
Consente di connettere il computer direttamente a un altro computer mediante la porta seriale, parallela o a infrarossi o di impostarlo per consentire la connessione di altri computer.
< Indietro
Avanti >
Annulla

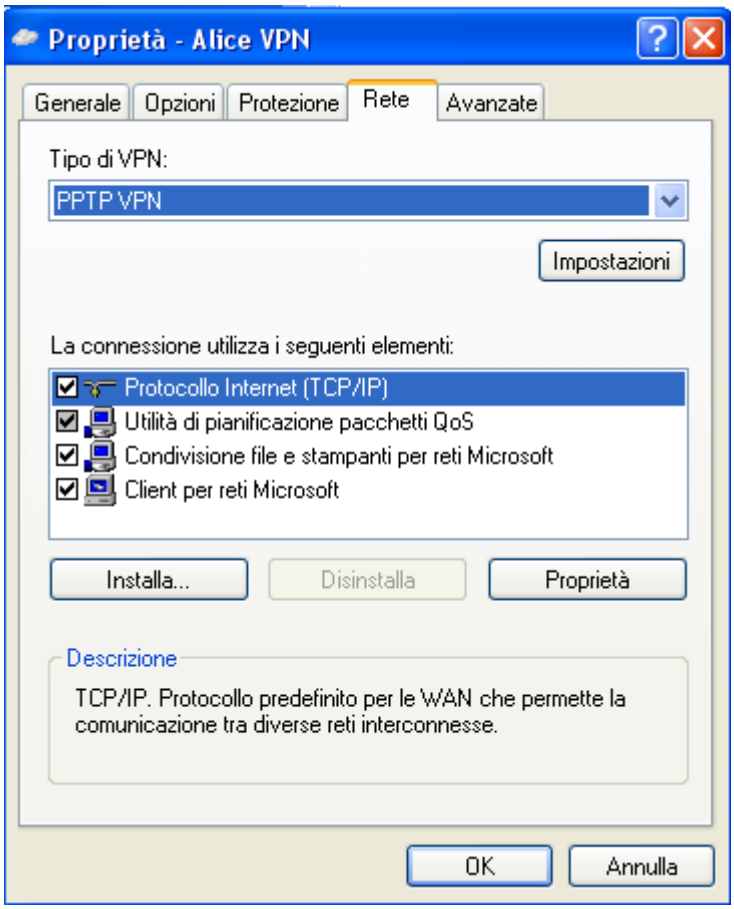

Creazione guidata nuova connessione
Connessione di rete
Scegliere la modalità di connessione alla rete aziendale.
Crea la seguente connessione:
Connessione remota
Consente di connettere il computer alla rete mediante un modem e una normale linea telefonica oppure mediante una linea ISDN.
Connessione VPN
Consente di connettere il computer alla rete mediante una connessione VPN (Virtual Private Network) su Internet.
< Indietro
Avanti >
Annulla



E’ necessario inserire l’IP privato dell’I-Storm Router ADSL.



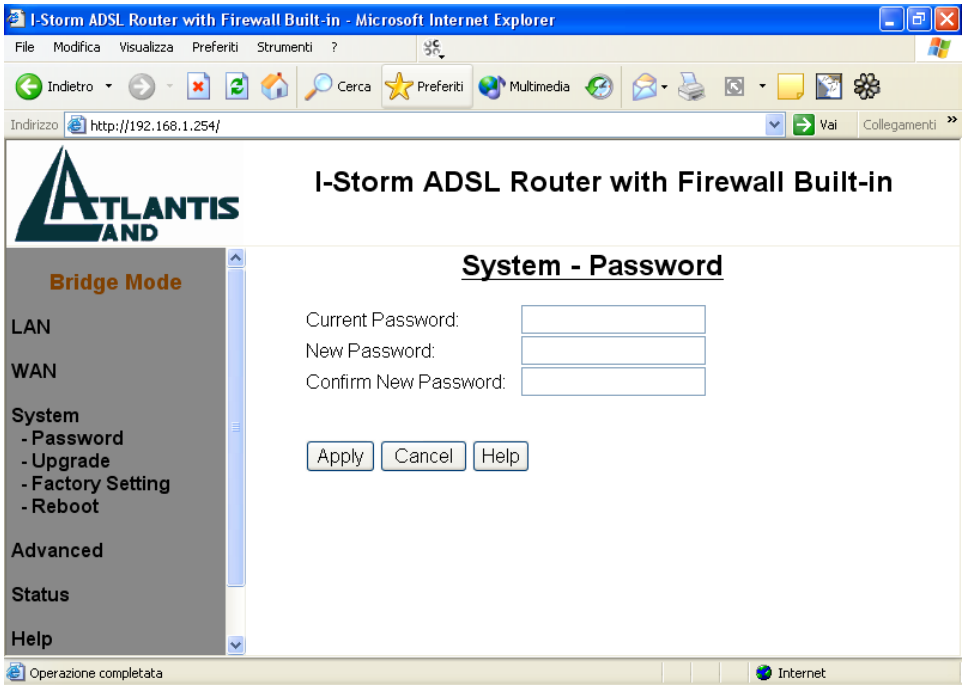
E' importante stabilire che la VPN sia di tipo PPTP.



Nel protocollo TCP/IP metterete il PC settato come client DHCP in modo che l'indirizzo IP, DNS gli venga fornito dal server dell'ISP. In questa modalità l'indirizzo IP pubblico viene associato direttamente al PC pertanto potrete utilizzare alcune particolari applicazioni che non funzionano attraverso il NAT. Il problema è che il PC è esposto è direttamente raggiungibile dall'esterno e non può beneficiare né della protezione offerta dal NAT né del Firewall.
Potrebbe essere necessario utilizzare particolari settaggi (PAP, abilita Estensioni LCP) per il corretto funzionamento della VPN.

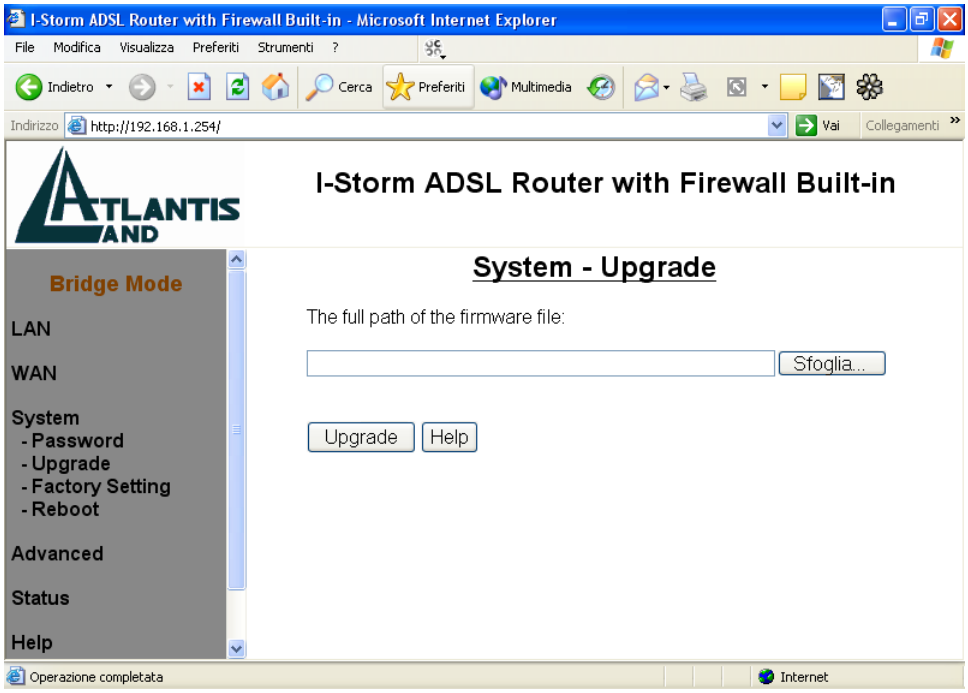
3.5.3 System

Password



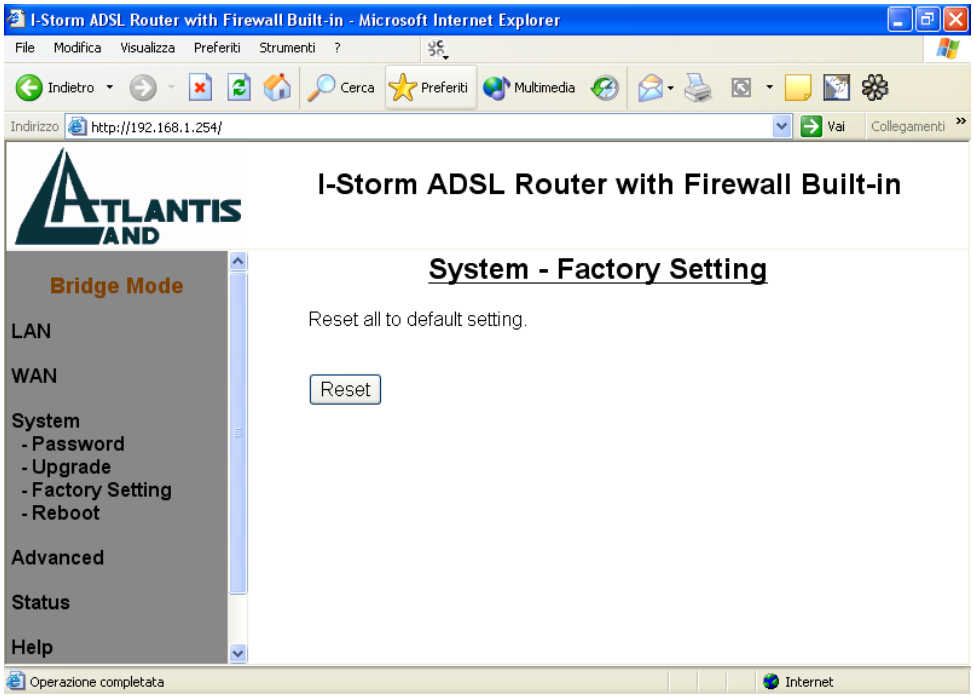
Le impostazioni di default non comprendono alcuna password. E' consigliabile cambiare tale settaggio al fine di evitare spiacevoli intrusioni. E' necessario conservare la nuova password in un posto sicuro, in quanto **non è possibile in alcun modo** (se non rivolgendosi ad AtlantisLand spa ed avendo **l'indirizzo MAC del Router**) **accedere (via web) al Router ADSL qualora venga persa**. La password può essere lunga sino ad 8 caratteri alfanumerici (accertarsi che la posizione del Caps Lock sia off)

Upgrade



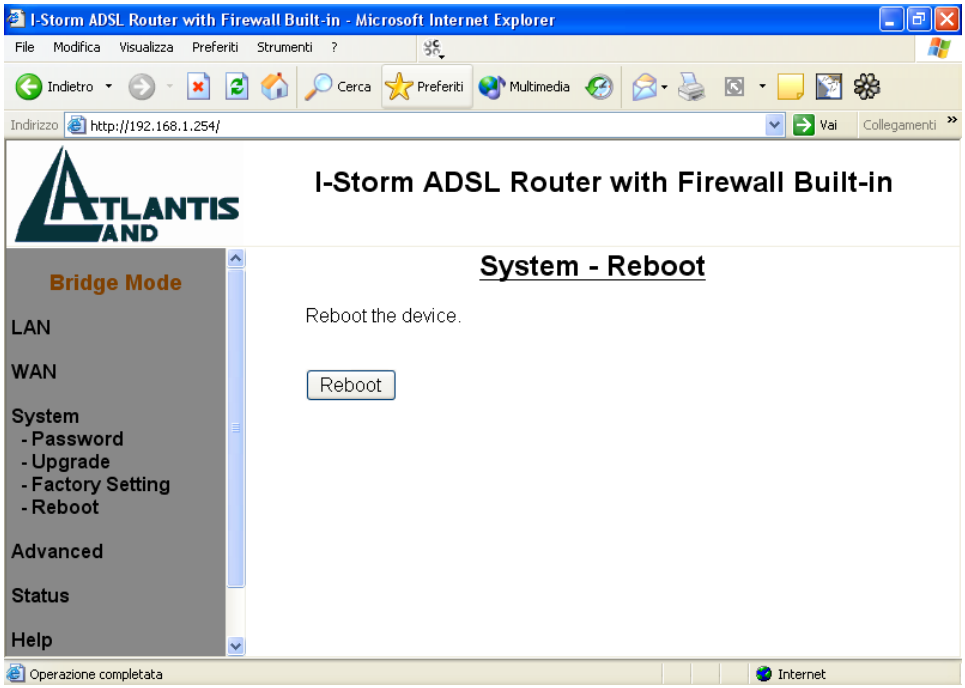
Per effettuare l'upgrade del firmware del Router ADSL è necessario anzitutto scaricare dal sito www.atlantisland.it o www.atlantis-land.com (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punto, sotto il menù **System** nel Menù principale, alla voce **Upgrade** e premere poi il tasto **Sfoglia** ed indicare il path dove si è messo il file del firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. **E' opportuno non staccare, durante la fase di upgrade, il Router ADSL dalla presa elettrica**. Completata la procedura l'I-Storm ADSL Router si resetterà automaticamente e inizierà a funzionare col nuovo firmware.

Factory Setting



Se per necessità si desidera reimpostare l'I-Storm ADSL Router con la configurazione di default (perdendo tutti i settaggi inseriti) sarà sufficiente accedere, sotto il menù **System** nel Menù principale, alla voce **Factory Setting** e premere poi il tasto **Reset.** I valori della configurazione di default sono riportati nella sezione **3.2** di questo manuale.

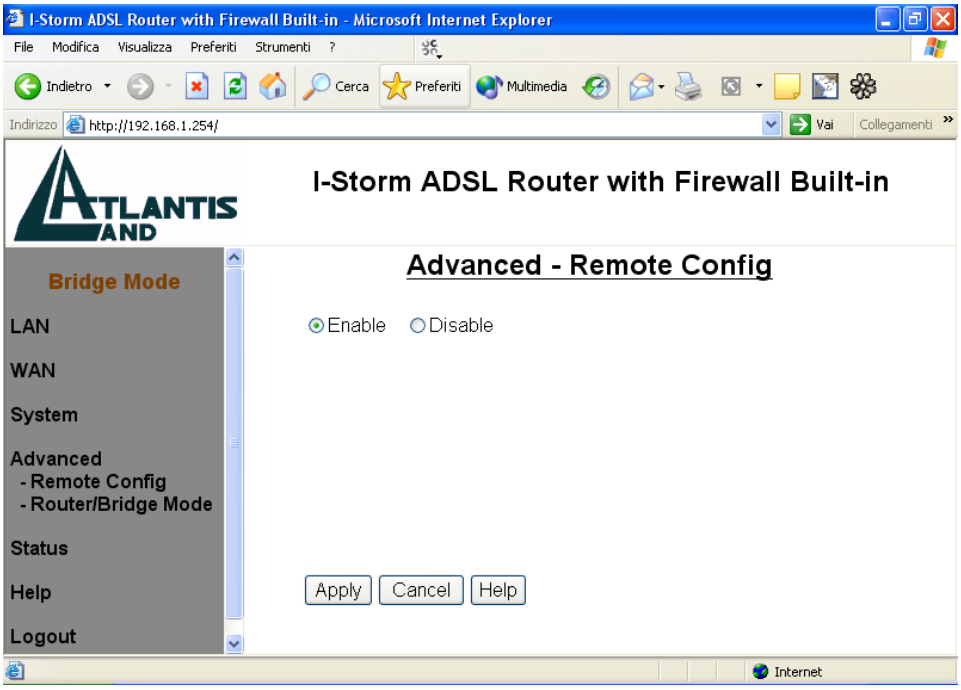
Reboot



Qualora il dispositivo smetta di rispondere o funzionare è possibile risolvere il problema accedendo, sotto il menù **System** nel Menù principale, e cliccare la voce **Reboot.** Apparirà una finestra in cui un timer vi aggiornerà sul tempo necessario alla riconnessione.

3.5.4 Advanced

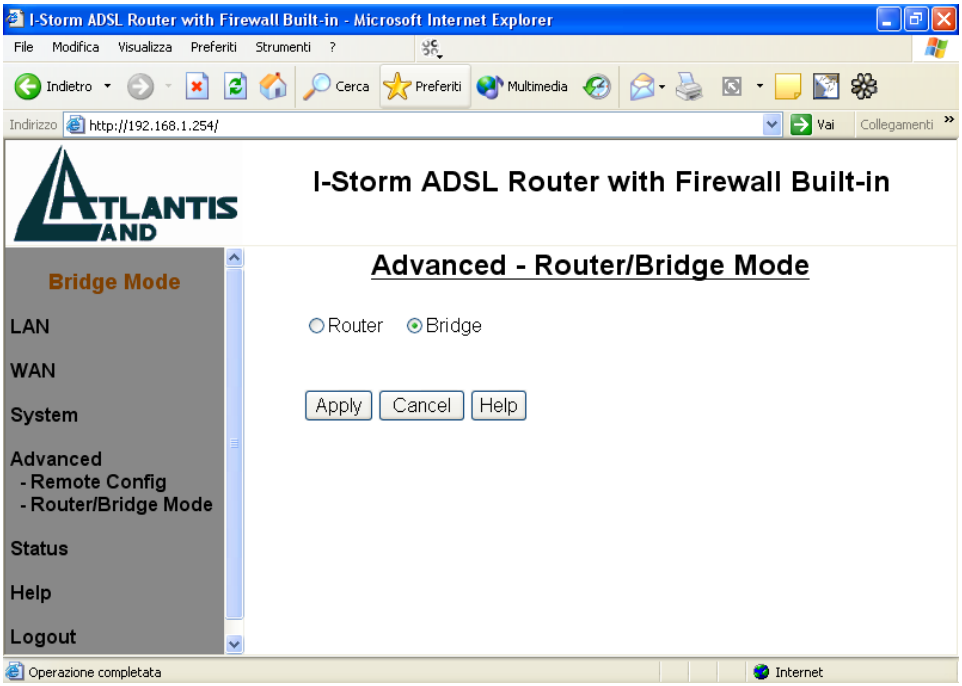
Remote Config



Per accedere alla configurazione remota digitare nell'URL del browser la seguente stringa:*http://Indirizzo WAN IP, dove WAN IP* è l'indirizzo IP pubblico del Router ADSL.

Scegliere Enable se si desidera configurare il Router ADSL da un qualsiasi PC collegato in Internet tramite un browser WEB.

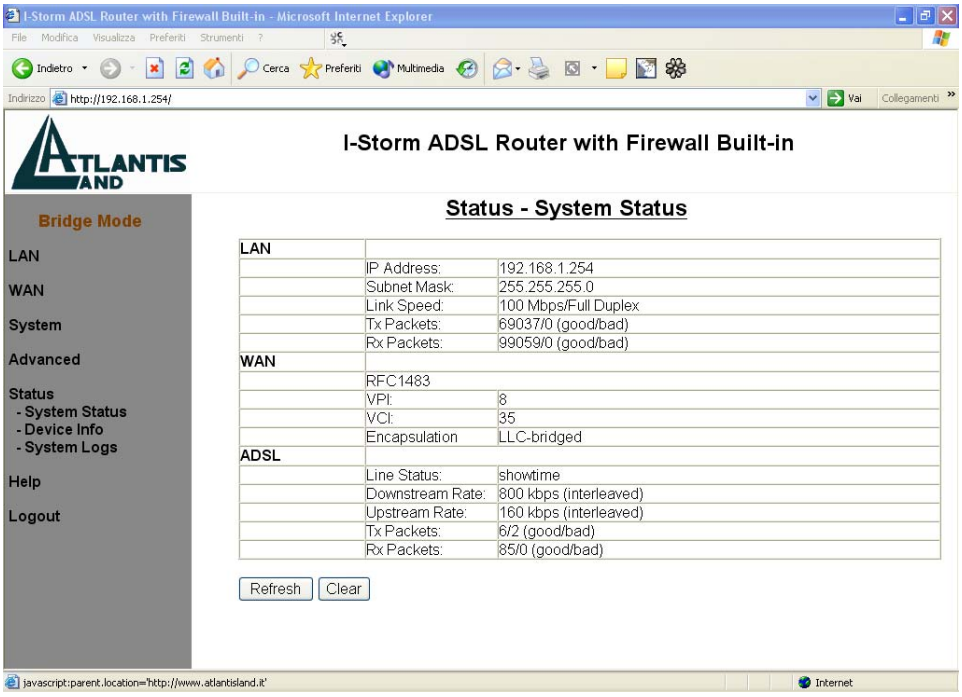
Router/Bridge Mode



E' possibile switchare la modalità di funzionamento del Router ADSL.

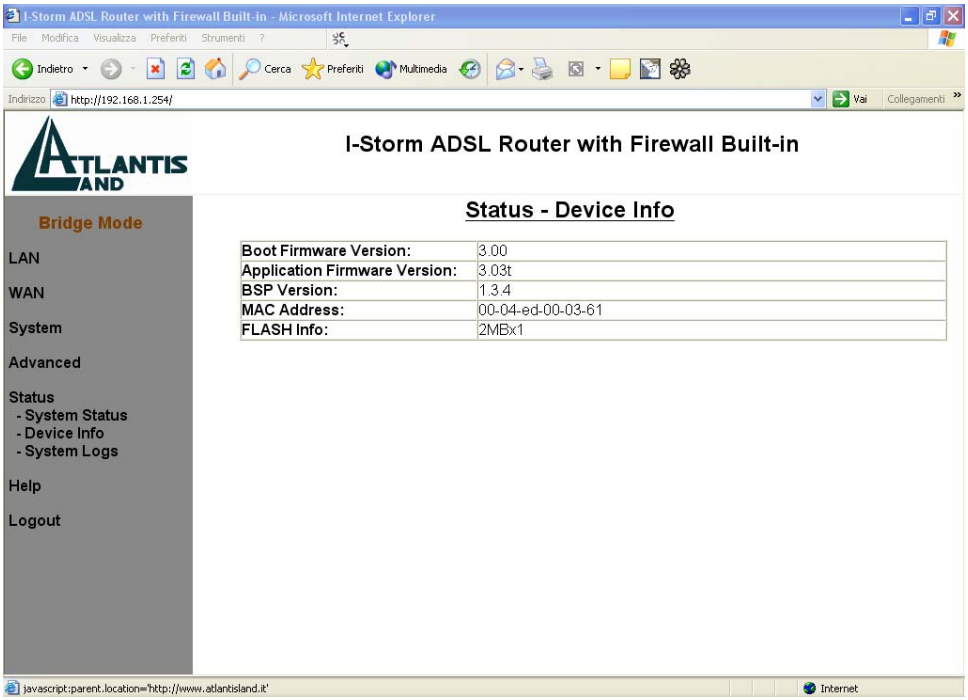
3.5.5 Status

System Status



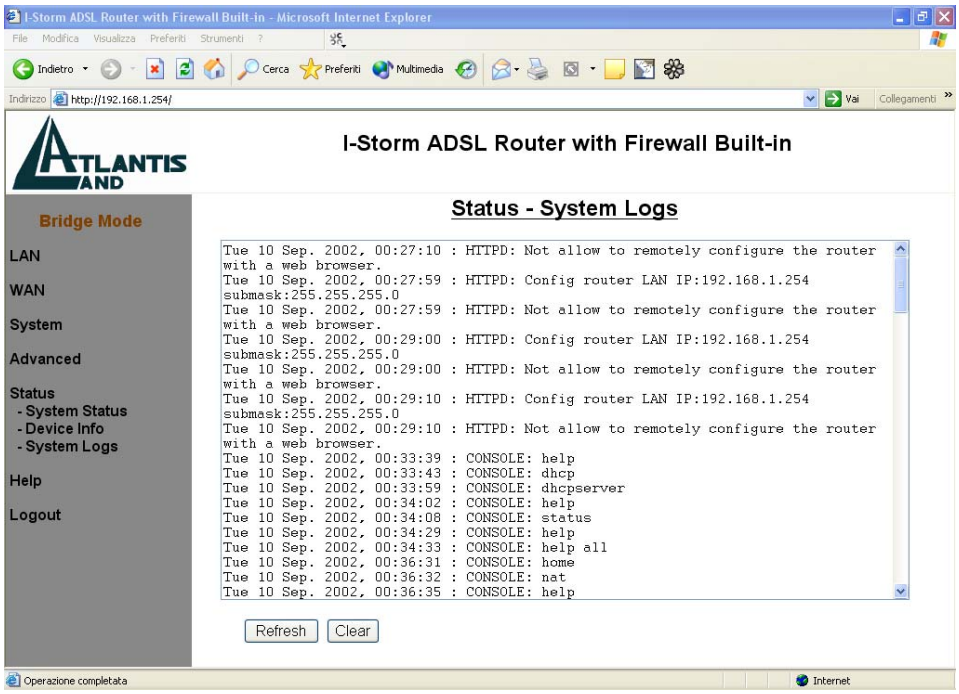
Mostra tutta una serie di informazioni sulla LAN, WAN e lo stato della connessione ADSL.
Questa pagina viene aggiornata ogni 15 secondi, cliccando sul bottone di REFRESH si otterrà invece un aggiornamento istantaneo.

Device Info



Mostra le versione di FirmWare ed l'indirizzo MAC del Router ADSL.

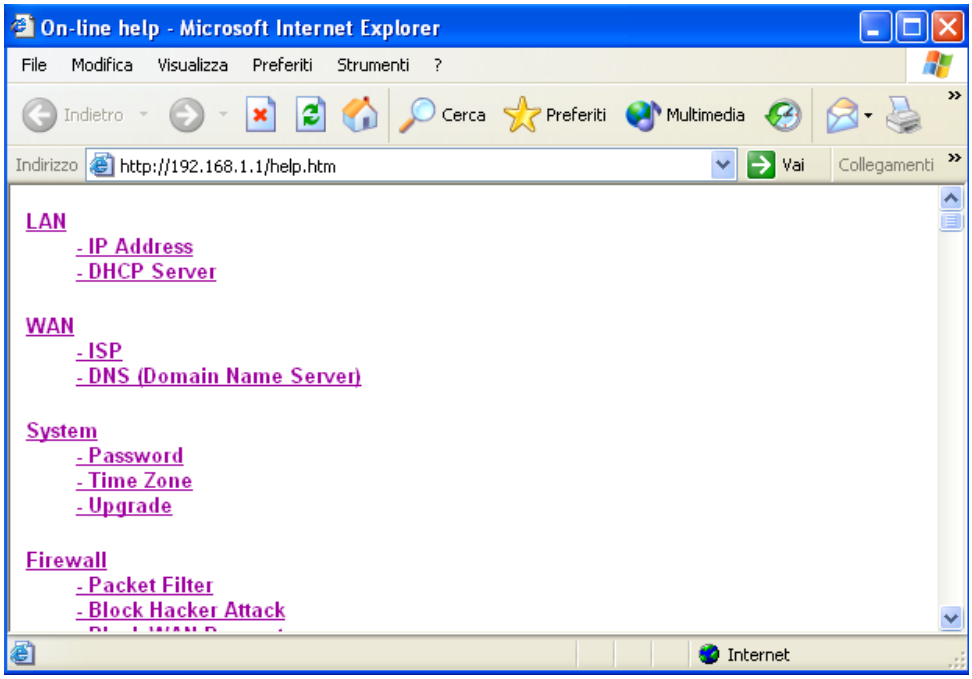
System Logs



Mostra tutte le informazioni storiche relative ai system logs.

Refresh / Clear: Cliccare su **Refresh** per vedere le ultime informazioni del system logs oppure cliccare su **Clear** per cancellare tutte le informazioni relative al system logs mostrate sullo schermo.

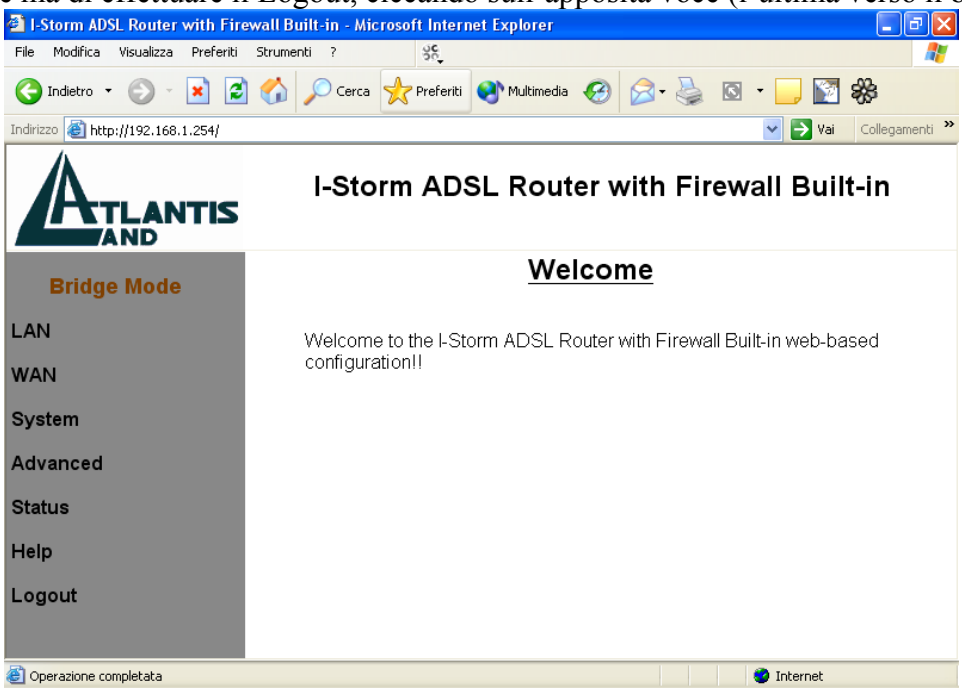
3.5.6 Help



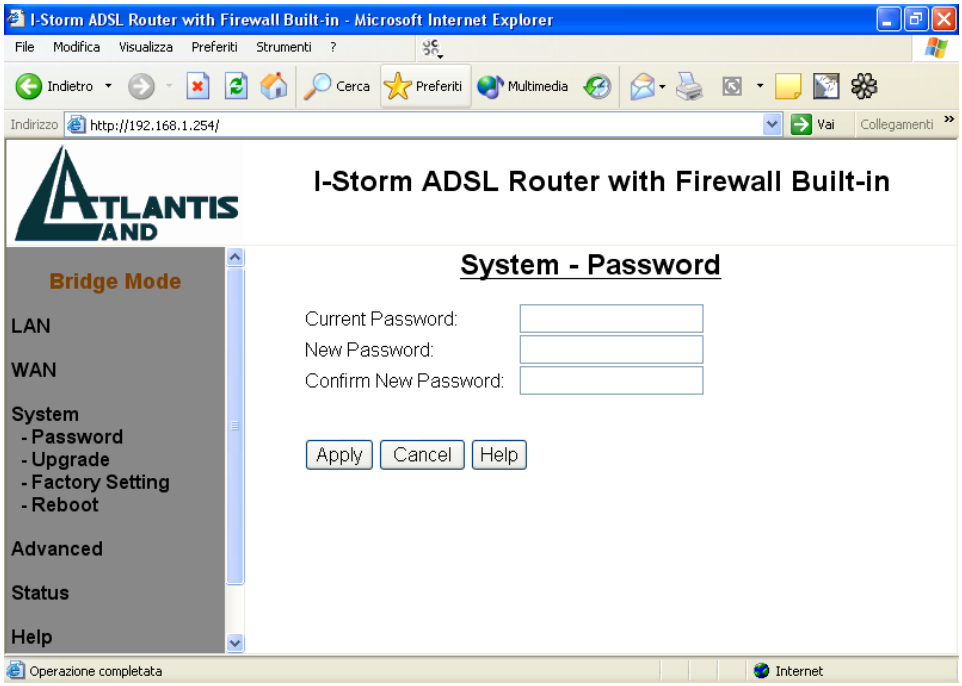
Premendo il bottone HELP, indipendentemente dalla sezione, vi apparirà un breve aiuto che vuole essere non un sostitutivo di questo manuale ma solo un promemoria delle varie voci che troverete nella configurazione dle Router ADSL.

3.5.7 Logout

Per uscire dalla configurazione del Router ADSL si consiglia di non chiudere il browser semplicemente ma di effettuare il Logout, ciccando sull'apposita voce (l'ultima verso il basso).

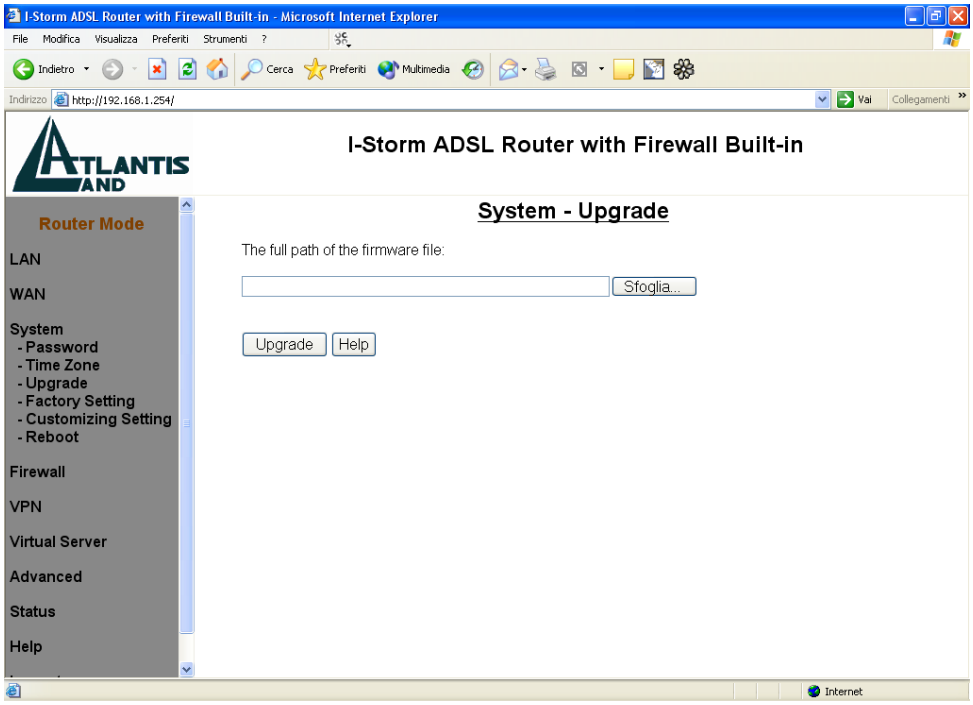


3.6 Cambiare la Password



Le impostazioni di default non comprendono alcuna password. E' consigliabile cambiare tale settaggio al fine di evitare spiacevoli intrusioni. E' necessario conservare la nuova password in un posto sicuro, in quanto **non è possibile in alcun modo** (se non rivolgendosi ad AtlantisLand spa ed avendo **l'indirizzo MAC del Router**) **accedere (via web) al Router ADSL qualora venga persa**. La password può essere lunga sino ad 8 caratteri alfanumerici (accertarsi che la posizione del Caps Lock sia off).

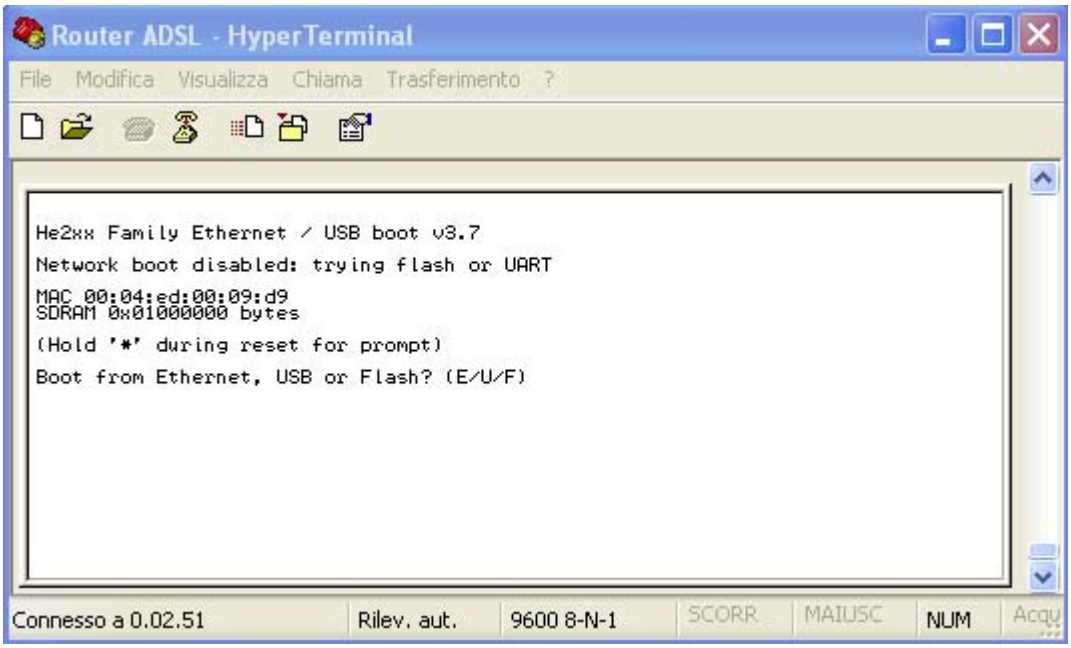
3.7 Firmware Upgrade



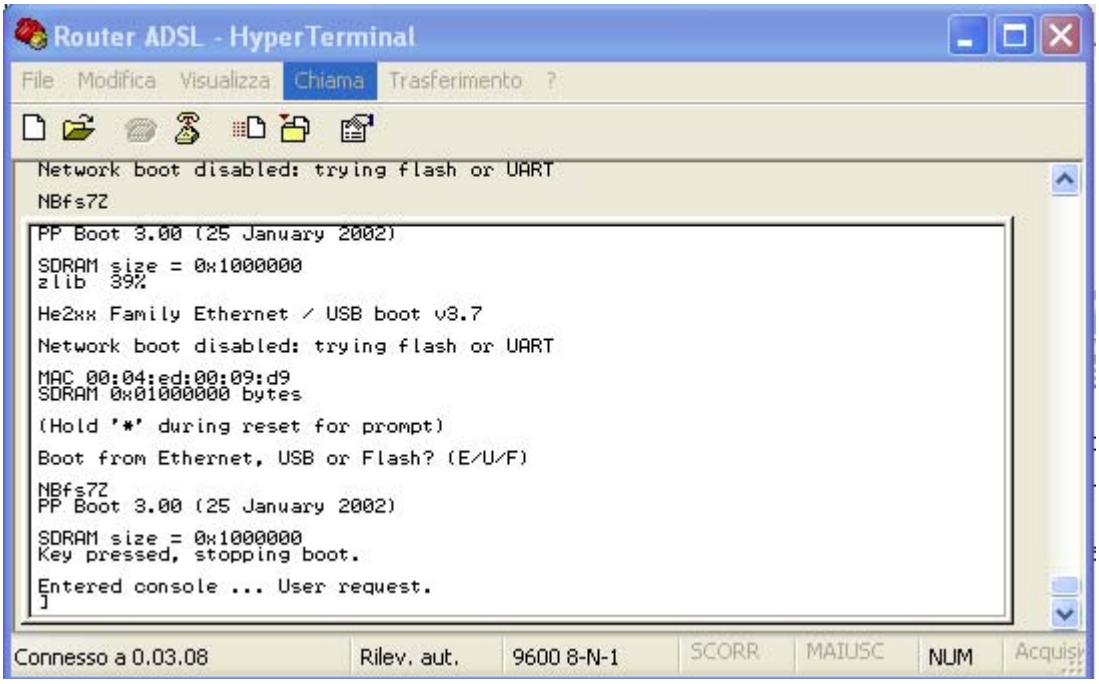
Per effettuare l'upgrade del firmware del Router ADSL è necessario anzitutto scaricare dal sito www.atlantisland.it o www.atlantis-land.com (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Accedere a questo punti, sotto il menù **System** nel Menù principale, alla voce **Upgrade** e premere poi il tasto **Sfoglia** ed indicare la path dove si è messo il file del firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento. **E' opportuno non staccare, durante la fase di upgrade, il Router ADSL dalla presa elettrica**. Completata la procedura l'I-Storm ADSL Router si resetterà automaticamente e inizierà a funzionare col nuovo firmware. Dovrebbero essere conservati i settaggi impostati precedentemente, sebbene a titolo cautelativo si consiglia di salvarli opportunamente.

3.8 Ripristino del Firmware

Questa procedura consente il ripristino del firmware del Router qualora qualcosa sia andato male durante la procedura di update o qualora si sia sprogrammata la memoria flash a causa di scariche elettriche provenienti, in massima misura (sono meno probabili quelle sul cavo Lan), tanto dalla rete elettrica quanto da quella telefonica. A tal fine vi invitiamo di dotarvi degli apparati adeguati per evitare eventuali guasti (**i fulmini e/o scariche elettriche non sono coperte da garanzia**). Preparare il Router collegando il cavo Lan ed il cavo seriale al PC, non collegarlo invece né alla rete elettrica né all'ADSL. Lanciare Hyperterminal sul Pc (leggere la sezione successiva per maggiori dettagli), scegliere la porta **Com** su cui è collegato il Router ed immettere poi i seguenti settaggi (**bit per secondo=9600, Bit di dati=8, Parità=Nessuno, Bit di Stop=1, controllo di flusso=Nessuno).** A questo punto tenete premuto il tasto **Shift** + * e, collegato il cavo elettrico al Router, dovrebbe apparirvi un'immagine come quella da foto allegata in cui potrete leggere l'indirizzo MAC (prendetene nota).

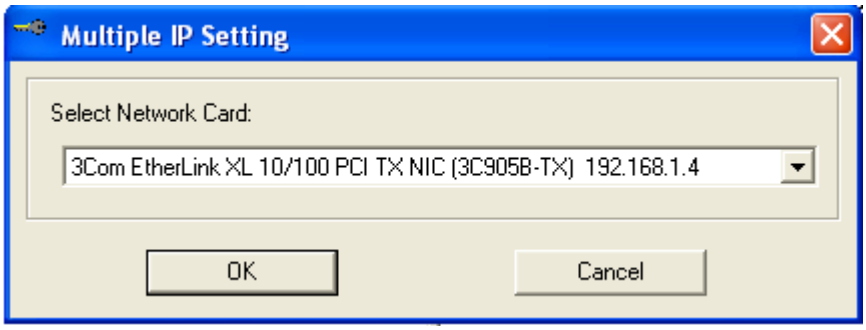


A questo punto premete **Shift+f** ed immediatamente lo **spazio,** dovrebbe apparirvi una parentesi quadra come prompt "]" .Se questo non è apparso ripetete l'operazione (non occupandovi di prendere il MAC) dall'inizio (uscite dalla connessione seriale, spegnete il Router, rilanciate la connessione seriale ed accendetelo e premete **Shift**+*, poi non appena appare Boot From…..premete **Shift+f** e immediatamente dopo lo **spazio**). Dovrebbe apparirvi un'immagine come da foto (se non appare ripete la procedura), se prima il Router si resettava continuamente adesso dovrebbe smettere.



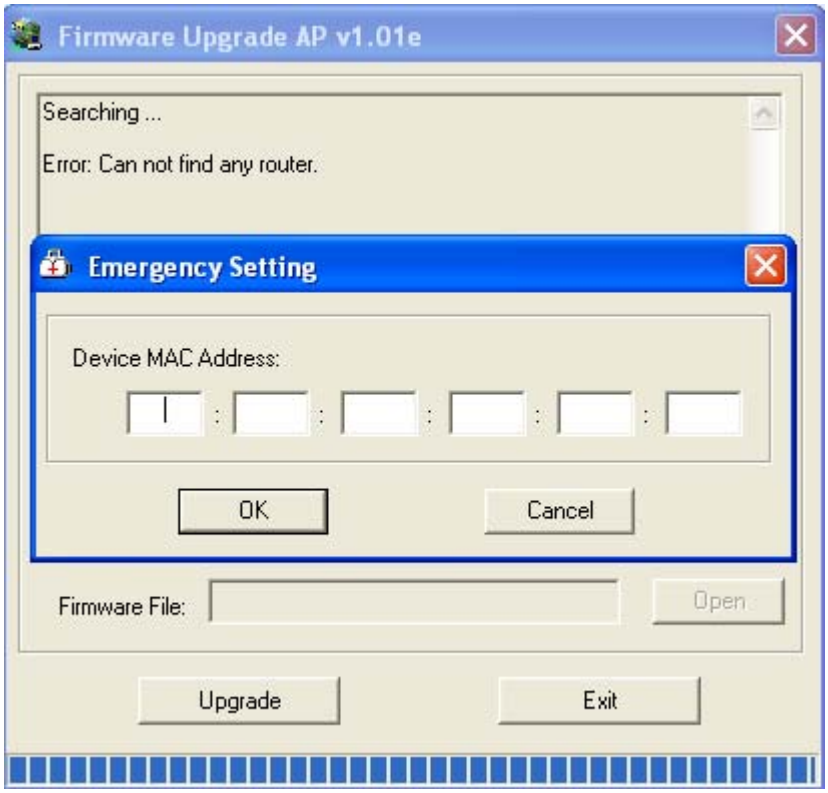
Digitate poi **configeeprom serialboot ethernet** e premete invio. Spegnete il Router staccando il cavo di rete elettrica e lasciate attiva la connessione seriale.

Lanciate **FWUP.exe** presente nella cartella **recovery** del CDROM allegato oppure richiedibile all'assistenza tecnica.

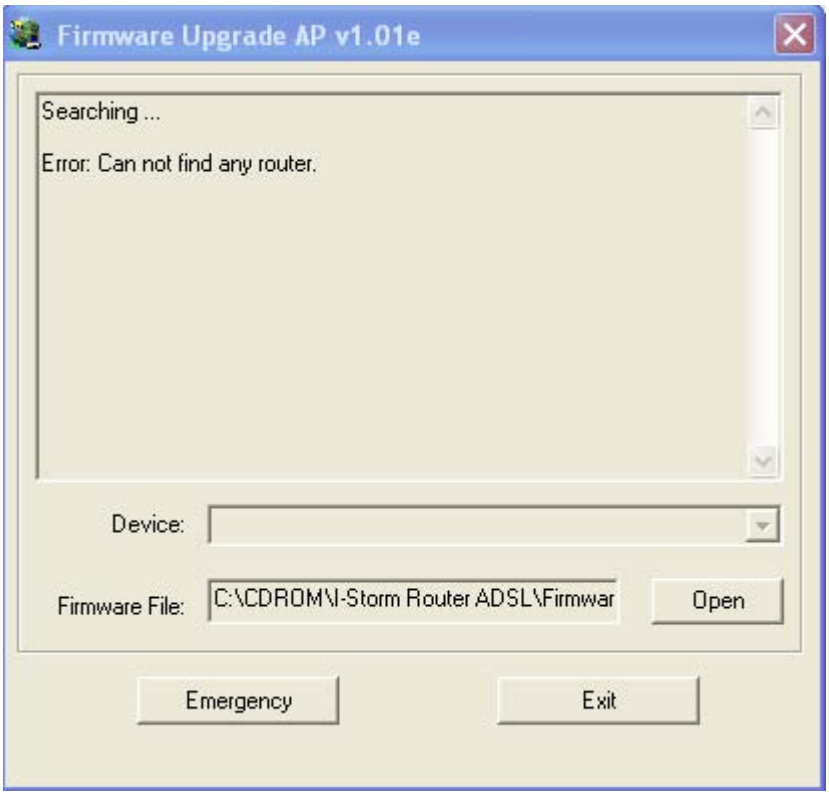


Scegliere la scheda di rete del proprio PC (**che dovrà avere necessariamente un IP fisso**).

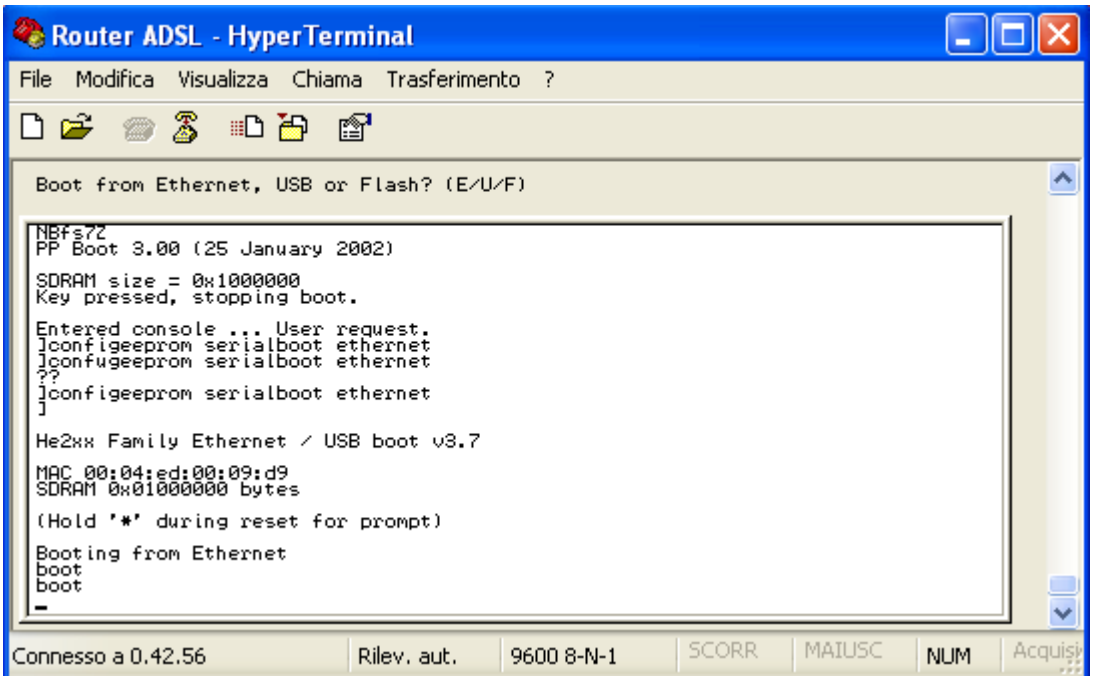
Fatto questo introducete nella figura il MAC preso precedentemente (vedrete solo caratteri maiuscoli, è normale). Premete **OK**.



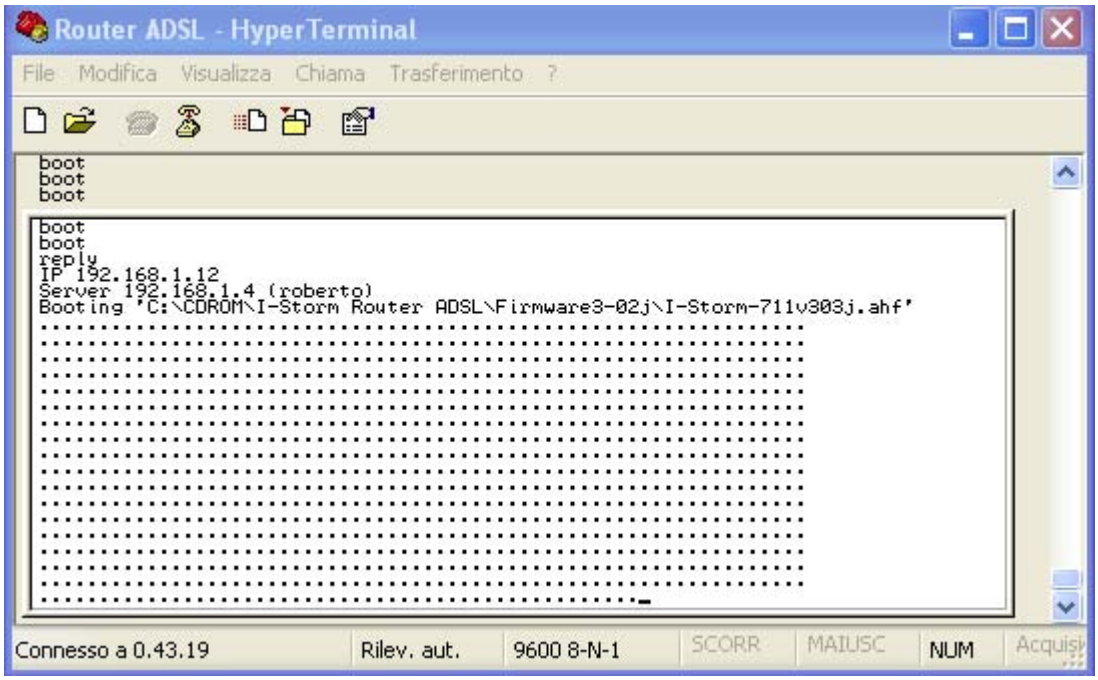
Premere **Open,** indicare il percorso in cui è presente il file Firmware di ripristino (**non è lo stesso usato per l'upgrade via WEB, non vano assolutamente scambiati**). Evidenziare in basso All Files e premere **apri**. Dovreste vedere l'immagine di sotto:



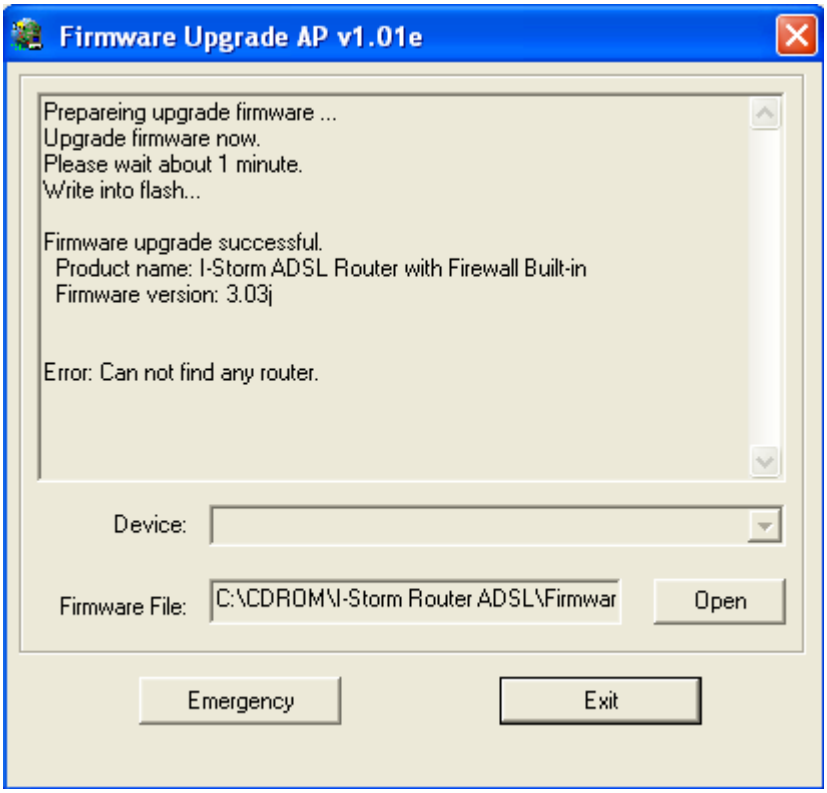
A questo punto scollegate il Router dalla corrente elettrica e poi ricollegatelo, dovreste vedere l'immagine di sotto (apparirà la scritta Boot continuamente mentre lampeggerà la luce ACT) ed immediatamente premete sul tasto Emergency .



Dovreste vedere un'immagine del genere (quella sotto) nella console di hyperterminal:



Terminata la procedura di update il Router risulterà perfettamente funzionante. Aspettate comunque di vedere l'immagine sotto che vi indicherà il corretto termine dell'operazione. Qualora non partisse l'upgrade automatico ma nella schermata della connessione seriale comunque è presente la scritta boot riprovare a premere il tasto Emergency.



3.9 Console e/o Telnet

E' possibile configurare il Router ADSL sia tramite Telnet (la password è:" **password** ") che tramite Console. Per la configurazione tramite Telnet andare nel prompt dei comandi Configurazione tramite Hyperterminal su ambienti Windows e digitare **telnet <indirizzo Lan IP>** e premere invio, introdurre la password.

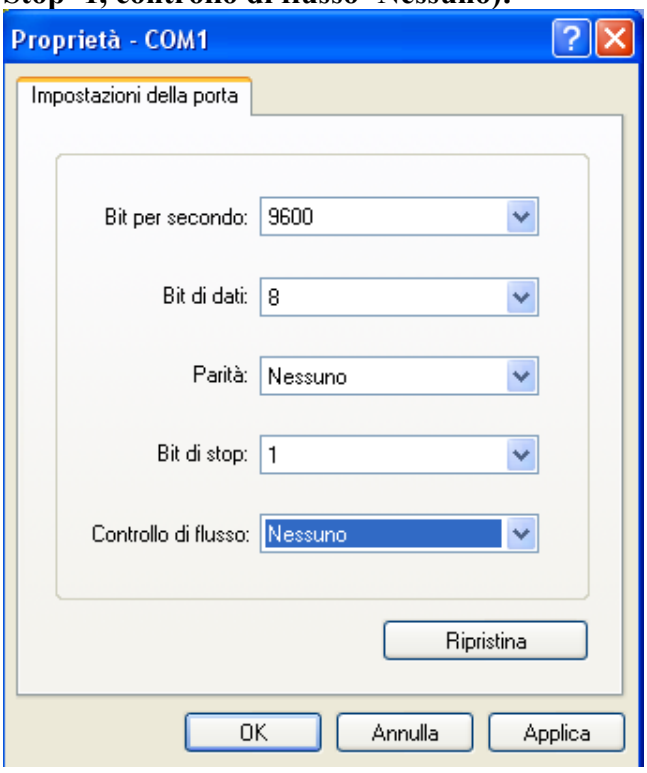
1-Lanciare Hyperterminal o qualsiasi altro programma di emulazione terminale (le istruzioni seguenti si riferiscono a hyperterminal).

In XP, ad esempio, andare su Start-tutti programmi-accessori-comunicazioni-hyperterminal

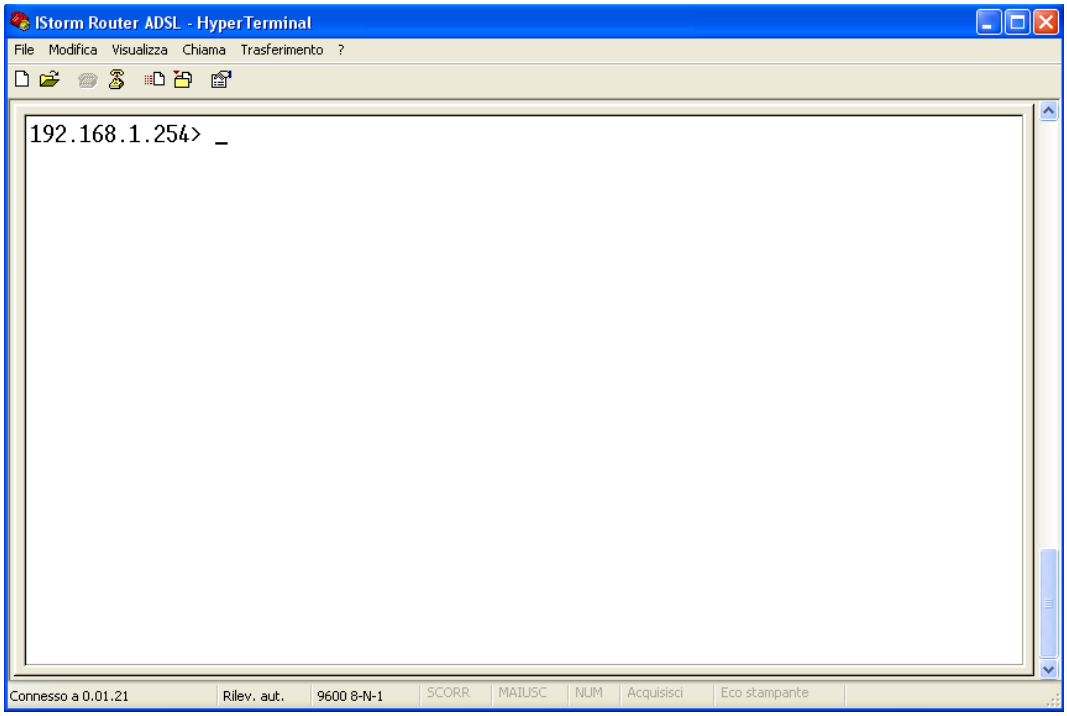
2-Introdurre il nome da dare alla connessione e premere OK.

3-Scegliere la porta COM cui è collegato l'I-Storm ADSL Router

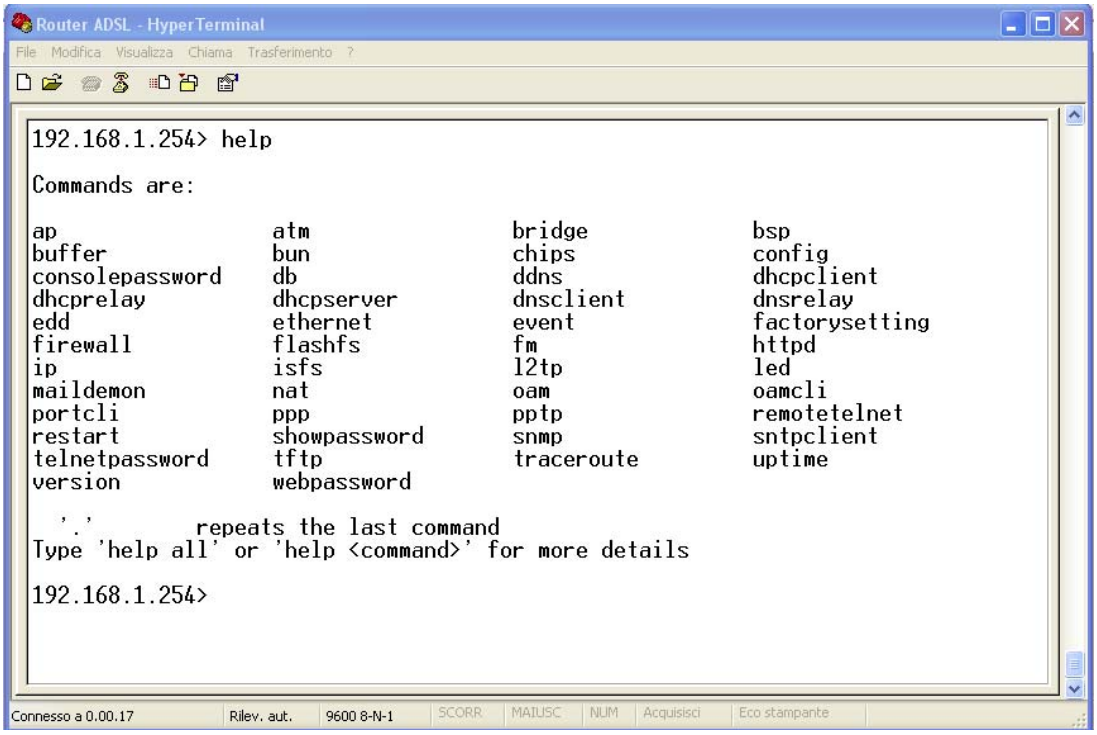
4-Inserire i settagli come da figura (**bit per secondo=9600, Bit di dati=8, Parità=Nessuno, Bit di Stop=1, controllo di flusso=Nessuno):**



Premere su Applica e poi OK.
Vi troverete a questo punto dopo aver premuto INVIO ed aver introdotto la password ("**password**") nella console dell'I-Storm Router ADSL.



A questo punto apparirà l'indirizzo LAN del Router ed un cursore lampeggiante. Utilizzando il comando **help** seguito dal tasto invio è possibile vedere la lista di tutti i comandi disponibili. Vi apparirà il seguente elenco (può variare a seconda del Firmware installato):



Digitando il nome del comando (se riferito ad un processo) seguito da invio e poi digitando **help all** potremo vedere tutti i comandi relativi all'opportuno processo. Per tornare alla root sarà sufficiente

digitare **home** seguito da invio. Alcuni comandi invece (quelli non riferiti ad un processo) eseguono immediatamente un'azione. Di questa categoria fanno parte:

restart (effettua il restart del Router)

uptime (mostra il tempo dall'ultima accensione o restart)

telnetpassword (consente di cambiare la password per l'accesso telnet, chiederà prima la vecchia)

webpassword (consente di cambiare la password per l'accesso web, chiederà prima la vecchia)

consolepassword (consente di cambiare la password per l'accesso console, chiederà prima la vecchia)

showpassword (mostrerà la password telnet e web)

remotetelnet [yes/no](consente di selezionare l'accesso telnet da remoto)

Processo IP

Vediamo adesso un esempio di processo. Digitando **ip** e premendo invio (dalla root) entreremo nel processo IP. Qui digitando **help** (seguito da invio) potremo vedere tutti i comando disponibili nel processo. Digitando **help all** (seguito da invio) potremmo vedere la sintassi di tutti i comandi del processo. Digitando invece **help + comando** (seguito da invio) potremmo vedere la sintassi riferita allo specifico comando. Per cambiare l'indirizzo IP è sufficiente digitare **enable ethernet** [nuovo IP] (seguito da invio). Potremmo accorgerci del cambiamento guardando la linea del cursore che adesso evidenzierà il nuovo indirizzo IP. Per cambiare ad esempio l'MTU dei pacchetti sull'interfaccia è sufficiente digitare **enable device ethernet mtu 1400 192.168.1.5** (seguito da invio, viene cambiato l'IP e settato l'mtu=1400). Premendo **device list** potremo controllare tutti questi nuovi settaggi. Entrate poi in **config** e salvate col comando **save.**

Processo BSP

Digitando **bsp** e premendo invio (dalla root) entreremo nel processo BSP. Al solito di digitando **help** (seguito da invio) potremo vedere tutti i comando disponibili nel processo. Premendo **line** (seguito da invio) potremo vedere tutti i parametri della linea (quali rumore, attenuazione). Premendo **perf** (seguito da invio) potremo vedere gli errori sulla linea. Premendo **channel** (seguito da invio) potremo vedere il data rate. Premendo **mode** (seguito da invio) potremo conoscere lo stato della linea. Il Router, grazie al supporto del protocollo G.994.1 (G.hs) riesce a scegliere il tipo di modulazione automaticamente. Potrebbe rendersi necessario forzare un tipo di modulazione in questo caso digitare il comando opportuno (**glite, gdmt, multi, ansi** seguito da invio) dopodiché digitare **down** (per far cadere la connessione) ed infine **up** (per ripristinarla con la nuova modulazione). Scoperta la modulazione corretta dell'ISP, andare in home poi nel processo **config** e digitare il comando **save**.

Processo NAT

Digitando **nat** e premendo invio (dalla root) entreremo nel processo NAT. Al solito di digitando **help** (seguito da invio) potremo vedere tutti i comando disponibili nel processo Premendo **interface** (seguito da invio) potremo vedere tutte le interfacce. Premendo **inbound list** (seguito da invio) potremo vedere a quali indirizzi IP privati sono reindirizzate le porte/protocolli. Per creare un Virtual Server è sufficiente digitare: **inbound add** [interfaccia] [numero porta]/[protocollo] [IP Lan]. Col comando **inbound list** è possibile vedere tutti i Virtual Server attivati. Premendo **inbound dolete** [n° regola] è possibile cancellare la singola regola di reindirizzamento, oppure premendo **inbound flush** è possibile cancellare tutte le regole.

Capitolo 4
Troubleshooting

Qualora il Router ADSL non funzionasse propriamente, prima di rivolgersi all'ISP, consultare questo capitolo.

Problemi alla partenza dell'I-Storm ADSL Router

Problema	Azioni correttive
Nessun LED è acceso quando si collega il Router ADSL alla rete elettrica.	Controllare la connessione tra l'alimentatore ed il Router ADSL, qualora il problema persistesse potrebbe essere un problema hardware. Rivolgersi, in questo caso, al supporto tecnico di AtlantisLand.

Ho dimenticato la Password

Problema	Azioni correttive
Qualora abbiate dimenticato la password per entrare nell'I-Storm Router ADSL oppure non ricordate più l'IP che gli avevate assegnato.	E' necessario collegare l'I-Storm Router ADSL ad un PC tramite il cavo seriale fornito. Lanciare sul PC un programma di emulazione terminale e scegliere i seguenti settaggi: **bit per secondo=9600, Bit di dati=8, Parità=nessuno, Bit di Stop=1, controllo di flusso=Nessuno** ed introdurre la password relativa al management da console che è "**password**". Qui (anzitutto potrete subito vedere l'IP del Router) digitando "showpassword" potrete vedere le password sia della parte WEB che della parte Console.
	Coi comandi **webpassword/telnetpassword** è possibile adesso cambiare le password di ingresso.

Non riesco ad entrare nel Router via WEB

Problema	Azioni correttive
Pur digitando l'IP del Router (192.168.1.254) non ottengo risposta, cosa posso fare?	Il problema potrebbe essere dovuto o ad un cablaggio errato oppure a causa di indirizzo IP del PC "inconsistente". Il Router viene fornito con un **cavo incrociato** tramite il quale va collegato o direttamente ad un PC oppure alla porta Uplink di un Hub/Switch. Qualora si usasse un cavo dritto (non fornito) è possibile connetterlo ad una qualsiasi porta di un Hub/Switch. Controllando i LED posti sul Router è possibile diagnosticare immediatamente lo stato del cablaggio. Nel caso di connessioni corretta il led Power=verde ed il led ACT=verde fisso. Bisogna attendere che il LED COL sia spento (qualora non accadesse e, si è certi del corretto cablaggio, spegnere il PC ed il Router e riaccenderli). A questo punto si è pronti per configurare il Router digitando il suo IP che di default è 192.168.1.254. Qualora non si riuscisse ancora ad entrare, è opportuno controllare l'indirizzo IP del PC e spostarlo sulla classe 192.168.1.x (ad esempio 192.168.1.1, subnet=255.255.255.0 e default gatewy quello del Router). Si potrebbe altresì spostare l'indirizzo IP del Router anche da console, per fare questo collegare il cavo RS232 fornito ad un PC e lanciare Hyperterminal, scegliendo la porta COM su cui è collegato il cavo seriale che collega il PC al router, con seguenti settaggi:**bit per secondo=9600, Bit di dati=8, Parità=nessuno, Bit di Stop=1, controllo di flusso=Nessuno** ed introdurre la password relativa al management da console che è "**password**". A questo punto per cambiare l'indirizzo IP è sufficiente digitare IP e premere invio per spostarsi nel processo IP. A questo punto digitare **enable ethernet** [nuovo IP] (seguito da invio). Potremmo accorgerci del cambiamento guardando la linea del cursore che adesso evidenzierà il nuovo indirizzo IP. Digitare **home** (seguito da invio), poi digitare **config**(seguito da invio) ed infine digitare **save** e premere invio per rendere permanenti le modifiche.

Problemi con l'interfaccia WAN

Problema	Azioni correttive
Fallisce l'inizializzazione della connessione PVC.	Assicurarsi che il cavo RJ11 sia connesso propriamente alla linea telefonica ed al Router ADSL. Il LED ADSL dovrebbe essere acceso fisso. Qualora lampeggiasse attendere che smetta, la connessione non è altrimenti realizzabile. Controllare i valori di VPI e VCI, il tipo di incapsulazione ed il tipo di modulazione (valori forniti dall'ISP). Effettuare il Reboot del Router ADSL. Andare (se si è in modalità Router) in System e poi nella sottosezione System status e qui sotto la sezione WAN controllare lo stato della connessione (il bottone deve essere sullo stato DISCONNECT, qualora così non fosse cliccarci sopra). Qualora il problema persistesse contattare l'ISP e verificare tali parametri.

Problemi con l'interfaccia LAN

Problema	Azioni correttive
Non posso fare il ping con alcun PC della LAN.	Controllare il LED Ethernet, nel pannello frontale. Tale LED dovrebbe essere acceso. Se così non fosse controllare il cablaggio.
	Verificare, nel caso in cui il LED sia acceso, che l'indirizzo IP e la subnet mask tra il Router ed i PC siano consistenti.

Problemi di Connessione ad un Remote Node oppure ad un ISP

Problema	Azioni correttive
Non riesce a connettersi ad un remote node o ad un ISP.	Fare riferimento alla ***sezione 3.4.8 "System Status"*** per verificare lo stato della linea.
	Nella ***section 3.4.7 "Remote Config"***, verificare Login e Password per la connessione col remote node.

Conflitto di indirizzi IP

Problema	Azioni correttive
Il PC visualizza un messaggio che informa sul conflitto dell'indirizzo IP.	La causa può essere un reboot del Router ADSL (se impostato come server DHCP) oppure da due o più PC che hanno lo stesso indirizzo. E' possibile lanciando l'utilità "**winipcfg**" controllare tutti i parametri (IP, Subnet, DG) ed eventualmente rinnovarli (se il PC è un client DHCP ed il Router funge da server DHCP). L'utilità "winipcfg.exe" è disponibile per Win95, 98 e ME. Per WinNT, Win2000 e WinXP utilizzare l'utility "**ipconfig**".

Il Router non riesce ad allinearsi?

Problema	Azioni correttive
Il Led ADSL continua a lampeggiare ed il Router non riesce ad allinearsi. Cosa posso fare?	E' necessario collegare l'I-Storm Router ADSL ad un PC tramite il cavo seriale fornito. Lanciare sul PC un programma di emulazione terminale e scegliere i seguenti settaggi: **bit per secondo=9600, Bit di dati=8, Parità=nessuno, Bit di Stop=1, controllo di flusso=Nessuno** ed introdurre la password relativa al management da console che è "**password**". Qui (anzitutto potrete subito vedere l'IP del Router) digitando BSP (seguito da invio) entreremo nel processo BSP. Premendo **mode** (seguito da invio) potremo conoscere lo stato della linea. Il Router, grazie al supporto del protocollo G.994.1 (G.hs) riesce a scegliere il tipo di modulazione automaticamente. Potrebbe rendersi necessario forzare un tipo di modulazione in questo caso digitare il comando opportuno (**glite, gdmt, multi, ansi** seguito da invio) dopodiché digitare **down** (per far cadere la connessione) ed infine **up** (per ripristinarla con la nuova modulazione). Scoperta la modulazione corretta dell'ISP, andare in home poi nel processo **config** e digitare il comando **save**.

Cos'è il NAT?

Quesito	Risposta
Cosa fa esattamente il NAT?	Nat significa Network Addsress Traslation (traslazione degli indirizzi di rete locale).E' stato proposto e descritto nell'RFC-1631 ed aveva, almeno originariamente, il compito di permettere uno sfruttamento intensivo degli indirizzi IP. Ogni strumento che realizzi il NAT è composto da una tabella costruita da coppie di indirizzi IP, uno della rete privata ed uno pubblico. Dunque c'è una traslazione dagli IP della rete privata a quelli pubblici ed il contrario. Il Router I-Storm ADSL supporta il NAT, pertanto con un'opportuna configurazione più utenti possono accedere ad Internet usando un singolo account (e un singolo IP pubblico).Il NAT consente a più utenti di accedere ad Internet al costo di un singolo account IP. Se gli utenti della LAN dispongono di indirizzi IP pubblici e possono pertanto accedere direttamente ad Internet (e fungere da server per determinati servizi) tale funzionalità dovrebbe essere disabilitata. Il Nat inoltre è una sorta di primo firewall che migliora la sicurezza della Lan locale. Andrebbe usata quando il traffico indirizzato verso Internet è una parte di quello che circola nella Lan locale, altrimenti tale funzionalità potrebbe degradare leggermente le prestazioni della connessione ad Internet. Tale funzionalità coesiste con la funzionalità Virtual Server, DMZ e DHCP. Il Nat manipola i pacchetti IP uscenti e ne cambia il campo "IP provenienza" sostituendo il mittente del pacchetto (in questo caso l'indirizzo IP il PC della Lan, che è un IP privato non valido in Internet) con l'IP pubblico dell'I-Storm ADSL Router. In questo modo tutti i pacchetti uscenti dal Router avranno nel campo mittente l'indirizzo IP pubblico del Router. Quando poi i pacchetti torneranno al Router (perché sono a lui indirizzati) questo in base a tabelle memorizzate provvederà al processo contrario e li spedirà al PC interessato nella Lan.

Percorso dei pacchetti

Problema	Azioni correttive
Non funziona il Server che ho settato su un PC.	Il Router ADSL I-Storm applica, ad ogni pacchetto, nell'ordine: Firewall (ogni pacchetto è processato a partire dalla prima regola. Una volta soddisfatta una regola si esegue l'azione appropriata altrimenti si procede alla regola seguente sino all'ultima regola, se nessuna precedente è soddisfatta). Virtual Server (i pacchetti entranti non "attesi" dal NAT, vengono smistati seguendo le regole, partendo dalla prima, presenti nel VS) DMZ (i pacchetti entranti non "attesi" dal NAT e non smistati dal VS sarebbero scartati se tale funzionalità fosse disabilitata) Affichè il Server funzioni bisogna accertarsi che nessun blocco antecedente al VS (Firewall) o DMZ (Firewall e VS) non operi in conformità. Settare il PC che funge da Server con un indirizzo IP privato fisso

Non funziona correttamente un'applicazione Internet

Problema	Azioni correttive
Alcune applicazioni, quando il Router fa NAT oppure è attivo il firewall, potrebbero non funzionare propriamente.	Il Router, tramite il NAT e/o il firewall, protegge la LAN isolandola dall'esterno e rifiutando tutti i tentativi di connessione generati dall'esterno. In Internet ogni servizio è associato ad una porta. Queste porte potrebbero essere chiuse per evitare che malintenzionati possano accedere alla LAN. Tuttavia può essere necessario, per il funzionamento di determinate applicazioni (ad esempio NetMeeting), che i tentativi di connessione generati dall'esterno su determinate porte siano rigirati ad un PC della LAN su cui il programma in questione sia in "ascolto". Consultare la sezione Virtual Server per avere maggiori dettagli. Le applicazioni che tipicamente dovranno essere configurate sono: **Alcuni Programmi di Email** **Alcuni Giochi Multi-Players** **Alcune Applicazioni Phone/Video Conferenza** Per trovare le porte da aprire per il corretto funzionamento dell'applicazioni solitamente la strada più breve è quella di consultare il sito web del produttore dell'applicazione. Resta inteso che in questo modo un solo PC della LAN (quello su cui saranno girate le opportune porte) potrà usare l'applicazione in questione.

Perché nonostante il VS alcune applicazioni non vanno?

Problema	Azioni correttive
Ho effettuato la rotazione delle porte col VS ma l'applicazione ancora non va, cosa posso fare?	Potrebbe rendersi necessario effettuare una DMZ verso il PC su cui si vuole far girare una particolare applicazione. Se ad esempio il PC in questione viene "chiamato" dall'esterno per la costruzione di una VPN bisogna necessariamente effettuare verso il suo IP privato una DMZ.

Perché nonostante la DMZ alcune applicazioni non vanno?

Problema	Azioni correttive
Pur utilizzando la DMZ l'applicazione non funziona ancora, cosa posso fare?	Nonostante le caratteristiche del Router alcune applicazioni potrebbero non funzionare perché non trasparenti al NAT (nemmeno effettuando una DMZ). In questo caso è possibile utilizzare il Router in modalità Bridge. Così facendo l'indirizzo IP pubblico del Router viene "dato" al PC che dunque potrà far funzionare tutte le applicazioni (come se il Router fosse un modem ADSL). Anzitutto abilitare la funzione Bridge, poi selezionare il protocollo **PPTP to PPPoA** per la connessione ADSL del Router e costruire una connessione VPN sul PC mettendo l'IP chiamato l'IP privato del Router, come username e password quelle della connessione all'ISP e scegliere la modalità PPTP. In questo modo ogni volta che effettueremo la chiamata VPN al Router, questo effettuerà un collegamento PPPoA (il tipo di protocollo che l'ISP utilizza per fornirvi il servizio) con l'ISP. In questo caso il router non è più server DHCP pertanto settate il PC con indirizzi IP statici privati e non come client DHCP. La VPN invece deve ottenere l'IP dal server (che è poi l'IP pubblico assegnatovi). Questo problema non si presenta dove il PC ha un indirizzo IP pubblico e pertanto non viene NATtato dal Router. E' altresì possibile usare il Router in PPTP to PPPoA non impostandolo come Bridge (per la costruzione della VPN seguire quello detto precedentemente), resta inteso che però un solo PC della LAN alla volta potrà accedere ad internet. E' possibile utilizzare il Router in modalità Bridge anche in RFC 1483 (in questa modalità, utilizzando un singolo PC è necessario avere un client PPPoE).

Le performance del Router non sono brillanti?

Problema	Azioni correttive
Le performance in download o in upload non sono allineate col tipo di contratto offerto dall'ISP.	Assicurarsi che il cavo ADSL sia (in ogni suo punto) ad almeno 30cm da qualsiasi alimentatore. Allontanare il Router da qualsiasi apparecchio che possa generare campi elettromagnetici (case con lo chassis aperto, monitor CRT) ed interferire. Qualora non si ottenesse il risultato sperato controllare il proprio contratto (vedere la banda minima garantita) ed eventualmente contattare l'ISP. Se i problemi continuassero, contattare l'assistenza tecnica di Atlantis Land spa.

Come posso controllare ogni accesso al Router?

Problema	Azioni correttive
Voglio impedire che chiunque acceda al Router da qualunque interfaccia?	Il router è configurabile (tramite porta Lan) tanto da locale tanto da remoto. Per impedirne l'uso non autorizzato è possibile cambiare tutte le password di accesso. Si ricorda che la configurazione di default ha come password: WEB=nessuna, Telnet=password, Console=password. Controllo remoto non attivo nè per la configurazione WEB nè per la Telnet. Per cambiare le password di accesso entrare nel router in modalità telnet e/o console e digitare uno dei seguenti comandi comandi:**consolepassword**, **telnetpassword** e **web password** (al solito andare nel processo config e digitare save). **Si ricorda che cambiando tutte e 3 le password (e perdendole) non sarà possibile accedere in alcun modo al Router.**

Come posso abilitare la funzionalità SPI?

Problema	Azioni correttive
Voglio accrescere la sicurezza dle Router abilitando la funzionalità SPI?	Tale funzionalità consente, utilizzando l'hardware del Router, di impedire ogni tipo di accesso indesiderato. Per abilitarla è sufficiente entrare nel router in modalità telnet e/o console e digitare:**firewall** (per entrare nel processo firewall) e poi **spi enable**. Digitando spi hash è possibile vedere i pacchetti su cui l'SPI è attivo. Con questa funzionalità attiva l'interà Lan sarà ulteriormente protetta poiché ogni pacchetto in transito viene esaminato a fondo e tutti i pacchetti di risposta vengono confrontati ed esaminati prima di essere inoltrati (di ogni pacchetto viene fatto una sorta di hash particolare che ne certifica l'autenticità). NB Alcune applicazioni internet potrebbero non funzionare correttamente con tale funzionalità attivata.

Cos'è il DHCP Relay?

Quesito	Risposta
Cos'è il DHCP Relay ed a cosa mi serve?	Settando questa funzionalità il servizio DHCP passa attraverso il Router I-Storm e raggiunge altri server che assegnano alla Lan i vari indirizzi IP. Se questa funzionalità non fosse disponibile questi PC sarebbero impossibilitati ad accedere al server DHCP. Al solito ogni PC che necessità di un indirizzo IP si mette in contatto con un server DHCP (in questo caso fuori dalla LAN) e da questo riceve: IP, Subnet. DG, DNS. Questi indirizzi IP sono dinamici, nel senso che hanno un tempo di validità. Scaduto questo termine il client DHCP ricontatterà il server per riottenere un nuovo IP.

Cos'è l'IDLE Time?

Quesito	Risposta
A cosa serve l'IDLE Time?	Il valore di default è 5 minuti. Il router ADSL stacca la connessione se non c'è traffico sulla connessione per 5 minuti (il che significa che nessun pacchetto, di alcun genere, è stato indirizzato dal Router verso Internet). E' possibile scegliere Always On per mantenere sempre alta la connessione (in PPPoA e PPPoE se tale modalità è abilitata il Routert ADSL alzerà nuovamente la connessione se questa dovesse cadere). Consigliamo di non utilizzare l'IDLE Time e mantenere il Router su Always ON a meno che non abbiate un abbonamento a tempo (attenzione in quel caso a monitorare la connessione che verrà ricostruita non appena un pacchetto sarà indirizzato, da un qualsiasi PC, verso un indirizzo diverso dalla subnet di appartenenza).

Perché il Router si connette automaticamente all'ISP?

Quesito	Risposta
Perché il Router si connette automaticamente all'ISP?	Il Router ADSL genera una connessione quando un PC della Lan invia un pacchetto (funzione di Dial on Demand) indirizzato ad un indirizzo IP differente da quello della sua classe di appartenenza (che è poi la subnet della Lan). Questo fenomeno deve essere controllato in caso di abbonamento non Flat e in condizioni di Idle Time attivato.

Cos'è un attacco Denial of Service?

Quesito	Risposta
Che caratteristiche ha un attacco Denial of Service?	Lo scopo di attacchi di questo tipo non è quello di cogliere informazioni particolari dalla vostra rete quanto piuttosto renderla inutilizzabile per un certo periodo di tempo. Più precisamente esistono 4 specifici tipologie di attacchi DoS. **1**-Attacchi che mirano all'esaurimento della banda, sono realizzabili in due modalità diverse a seconda di quanta banda abbia l'attaccante. Qualora la banda sia maggiore dell'attaccato può saturarlo diversamente può usare altri host che di fatto amplificano l'attacco. **2**-Attacchi che mirano all'esaurimento delle risorse. **3**-Attacchi contro difetti di programmazione, che mirano a sfruttare bug software o hardware. **4**-Attacchi DoS generici. Il Router può automaticamente accorgersi e bloccare un attacco di tipo DoS (Denial of Service) se questa funzione è attiva. Vengono riconosciuti oltre 15 tipi diversi di patterns (col firmware 3.02g) tra i quali: **IP Spoofing**, **IP with zero length, Ping of Death(Length>65535),Land Attack (Same source / destination IP address)**, **Sync flooding** **Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255), Snork Attack, UDP port loop-back, TCP NULL scan**, **Back Orifice Scan**, **Net Bus Scan TCP XMAS Scan**, **WinNuke Attack**, **IMAP SYN/FIN scan.**

Cos'è il DDNS?

Quesito	Risposta
A cosa serve il DDNS?	Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico. Ogni qual volta il Router si riconnettera, tramite il client incorporato, comunicherà al server DNS il nuovo indirizzo IP. Associando tale funzionalità con il Virtual Server è possibile ospitare un sito WEB sul proprio PC. I passaggi da seguire sono i seguenti: **1**-Registrare il proprio dominio gratuitamente e istantaneamente su www.dyndns.org, www.zoneedit.com. **2**-Configurare il client sull'I-Storm Router ADSL inserendo i campi appropriati (Domain Name, Username e Password) **3**-Predisporre il PC che deve fungere da server **4**-Configurare il Virtual Server affinché rigiri sull'indirizzo IP del PC (di sopra) predisposto le connessioni provenienti dall'esterno In questo modo ogni utente che voglia connettersi al vostro dominio interrogherà il server DNS che gli restituirà di volta in volta l'indirizzo IP assegnatovi dall'ISP. Usando la funzionalità di riconnessione (disponibile in PPPoA e PPPoE), qualora la connessione dovesse cadere, il Router la rialzerà immediatamente. In questo modo se il PC resta sempre acceso il server WEB è di fatto sempre raggiungibile (se si escludono problemi diversi).

APPENDICE A
Specifiche

Protocolli	IP, NAT, PPTP, ARP, ICMP, DHCP, PPPoE, PPPoA, IpoA, PPTP client, RIP1/2 e RFC1483
Porta LAN	RJ-45, 1 porta 10/100Base-T
Porta WAN	RJ-11, 1 ADSL porta
LED Indicatori	PPP, LAN-ACT, LAN-COL, ADSL, Power
Alimentatore	5V DC @1.5A
Potenza assorbita	< 6 watts
Conformità con	FCC part 15 Class B, VCCI, CE
Dimensioni Fisiche	212 x 142 x 38 mm^3 (L x P x A)
Peso	500g (circa)
Temperatura Operativa	Da 0℃ a 42℃
Temperatura supportata (non in funzionamento)	Da -10℃ a 70℃
Umidità Operativa	5-95% senza condensazione

APPENDICE B
Supporto Offerto

Qualora dovreste avere dei problemi con l'I-Storm Router ADSL consultare questo manuale. Molti problemi potrebbero essere risolti cercando la soluzione del problema nel Capitolo 4.
Per qualunque altro problema o dubbio (prima è necessario conoscere tutti i parametri usati dall'ISP) potete contattare l'help desk telefonico (**02/93907634**) gratuito di Atlantis Land che vi fornirà assistenza da lunedì a venerdì dalle 9:00 alle 13:00 e dalle 14:00 alle 18:00. Potete anche utilizzare il fax (02/93906161) la posta elettronica (info@atlantisland.it oppure tecnici@atlantisland.it).

AtlantisLand spa

Via Gandhi 5 Ing2,Scala A

20017 Mazzo di Rho(MI)

Tel: 02/93906085 (centralino), 02/93907634(help desk)
Fax: 02/93906161
Email: info@atlantisland.it oppure tecnici@atlantisland.it (mettere nell'oggetto il prodotto su cui si chiede assistenza)

WWW: http://www.atlantisland.it o www.atlantis-land.com